Sharing Information - Technology - Experience

CHIPS

Building Global Maritime PARTNERSHIPS

IN THIS ISSUE

INTERVIEWS WITH

VICE ADMIRAL HARRY B HARRIS Jr
CPNAV N6

VICE ADMIRAL H DENBY STARLING II
COMMANDER NETWARCOM

ITALIAN NAVY ADMIRAL LUCIANO ZAPPATA
ACT DEPUTY COMMANDER

REAR ADMIRAL JOHN M RICHARDSON
USJFCOM DIRECTOR STRATEGY AND POLICY DIRECTORATE

CREW OF FS TONNERRE
FRENCH NAVY'S COMMAND AND PROJECTION SHIP

CAPTAIN JACK L SOTHERLAND
BATAAN ESG/PHIBRON 2 COMMODORE

April - June 2009

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
01 JUL 2009	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
CHIPS - Building Global Maritime Partnerships	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Department of the Navy**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**UU**	**60**	

CHIPS
April - June 2009 | Volume XXVII Issue II

CHIPS is sponsored by the Department of the Navy Chief Information Officer (DON CIO) and the DON IT Umbrella Program Office, Space and Naval Warfare Systems Center Pacific.

CHIPS is published quarterly by the Space and Naval Warfare Systems Center Atlantic. USPS 757-910 Periodical postage paid at Norfolk, VA and at an additional mailing office. POSTMASTER: Send changes to CHIPS, SSC Atlantic, 9456 Fourth Ave., Norfolk, VA 23511-2130.

Submit article ideas to CHIPS at chips@navy.mil. We reserve the right to make editorial changes. All articles printed in CHIPS become the sole property of the publisher. Reprint authorization will be granted at the publisher's discretion.

Requests for distribution changes or for other assistance should be directed to Editor, CHIPS, SSC Atlantic, 9456 Fourth Ave., Norfolk, VA 23511-2130, or call (757) 443-0905; DSN 646. E-mail: chips@navy.mil; Web: www.chips.navy.mil.

Don't miss a single issue of CHIPS! To request extra copies or send address changes, contact CHIPS editors at chips@navy.mil or phone (757) 443-0905, DSN 646.

Cover Story: Building Global Maritime Partnerships - the U.S. Navy, working closely with government and nongovernment national and international organizations, is engaged worldwide fostering strong relationships, from African Partnership Station with USS Nashville (LPD 13) in Ghana to Southern Partnership Station with High speed vessel Swift (HSV 2) in South America, to improve maritime safety and security and ensure freedom of the seas.

In the photo above, Sailors aboard the amphibious transport dock ship USS Nashville (LPD 13) salute the Nigerian Navy frigate NNS Aradu (F 89) while pulling into Lagos Nigeria. Nashville is deployed as part of Africa Partnership Station, an international initiative, which aims to work cooperatively with U.S. and international partners to improve maritime safety and security on the African continent. U.S. Navy photo by Mass Communication Specialist 3rd Class Matthew Bookwalter.

Cover

UTAPHAO, Thailand (Feb. 27, 2008) Adm. Timothy J. Keating, commander of U.S. Pacific Command, is greeted by Royal Thai Navy pilots upon his arrival to Utaphoa. Keating met with Thai military leaders and government officials and emphasized the importance of the shared commitment to peace, stability and security throughout the region. Navy photo by Mass Communication Specialist 2nd Class Elisia V. Gonzales.

Navigation Guide

Features - Interviews with

In Every Issue

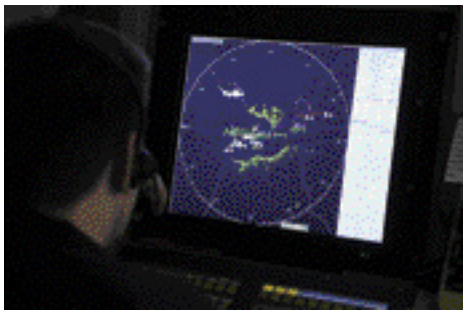
N W E S

Department of the Navy Policy

Information Sharing

Navy Network Enterprise

Maritime Technologies



Aboard the multipurpose amphibian FS Tonnerre, the French Navy's all-electric ship designed to operate far forward.

Training

Information Assurance

Workforce

Editor's Notebook

In this issue, we examine the enduring importance of maritime security to project forward presence; protect trade and shipping lanes; preserve national sovereignty; ensure regional stability; and prevent criminal activity and violent extremists' use of the maritime environment as a venue for attack or to transport contraband. Maritime security is an objective also prized by our closest allies and newest partners in maritime security operations.

Deputy Supreme Allied Commander Transformation Adm. Luciano Zappata refers to maritime security as "freedom of the seas," and in this issue, he discusses the need to expand maritime partnerships beyond traditional NATO partners. More and more countries are emerging to protect their vital interests at sea. We share the same challenges and must work within the same complex international political and legal framework to ensure maritime safety and security, Adm. Zappata said.

Sharing in the maritime security discussion are Capt. Jack L. Sotherland, commodore of the Bataan Expeditionary Strike Group and commander of Amphibious Squadron Two, and the commanding officer of FS Tonnerre, French Navy Capt. Edmond de Vigouroux d'Arvieu.

The Bataan ESG and Tonnerre underwent maritime security training in February. "No one navy can do it alone," Sotherland said. The U.S. Navy must take advantage of the strengths and expertise of allied partners, he said. Many of our allies like the English, Dutch and French, just to name a few, have hundreds of years of experience in working with other nations and cultures… Sotherland said that partner nations bring a different perspective and understanding to forming maritime coalitions.

In his interview, USJFCOM's Director for Strategy and Policy Rear Adm. John M. Richardson discusses the Joint Operating Environment which forecasts possible challenges and opportunities that will face the joint force in the future. Analysts predict that it will fall to the United States and its partner nations to protect and sustain the peaceful global system of interdependent networks of trade, finance, information, law and governance. So it is paramount that nations work together to ensure stability in the maritime environment.

Security operations and interoperability with partner nations would not be possible without robust command and control, and OPNAV N6 Vice Adm. Harry B. Harris and NETWARCOM Commander Vice Adm. H. Denby Starling II discuss strategy and policy initiatives that will strengthen the naval network environment for warfighting operations as well as business transactions.

In February, CHIPS joined Team SPAWAR in an exhibit at West 2009 in San Diego and the DON CIO at the DON IM/IT Conference held at the same time and location as West 2009. The DON IM/IT Conference was a great way to learn about new DON policy and projects and connect with colleagues.

See you at the East Coast DON IM/IT Conference, May 11-14, 2009, at the Virginia Beach Convention Center. The conference will be held at the same time and location as the Joint Warfighting Conference. Register for the DON IM/IT Conference by going to the DON CIO Web site: www.doncio.navy.mil.

Welcome new subscribers!

Sharon Anderson

Italian Navy Adm. Luciano Zappata

Aboard FS Tonnerre, Marines from the 22nd MEU prepare for the Composite Training Unit Exercise as part of the Bataan Expeditionary Strike Group with Tonnerre's officers and crew.

No one navy can do it alone... The U.S. Navy must take advantage of the strengths and expertise of allied partners ... They bring a different perspective and understanding to forming maritime coalitions.

U.S. Navy Capt. Jack L. Sotherland

MESSAGE FROM THE

DON CIO


Robert J. Carey

Information Sharing to Build Partnerships in Support of Maritime Domain Awareness

Our nation has set forth strategies to protect our homeland and the maritime domain that surrounds it. A key facet of these strategies is building partnerships. The Navy, Marine Corps and Coast Guard have partnered together to build our 21st century seapower.

Partnerships are being built across federal agencies and with state, local and tribal entities. Partnerships also expand globally with our NATO allies and other international partners.

Expanding cooperative relationships and developing partnerships with other nations contributes to the security and stability of the maritime domain for the benefit of all. All of these partnerships rely on the ability to share information.

In the Department of the Navy, our efforts are primarily focused on the maritime domain. Maritime Domain Awareness (MDA) is defined as "effective knowledge of all activities associated with the global maritime environment that could impact the security, safety, economy, or environment of the United States." Information sharing is a foundational tenet of MDA.

Recent piracy events challenge international security and impact the global economy. Combating these events has brought about a new requirement to interact and share information with a diverse set of partners outside our firewalls on a non-classified enclave. This has brought a new perspective and new challenges.

Truly successful information sharing requires a shift in the way we do business. The first and perhaps most difficult challenge is changing culture. We must move away from the "isolated need to know" and move to the "trusted need to share." As the Web 2.0 generation continues to pervade our workforce with their ingrained practice of constant collaboration and openness, this will also help shift our government culture toward one that readily fosters and benefits from information sharing.

A second challenge is the fact that existing information sharing policies are not always adequate. In addition to following all civil liberty, regulatory and legal guidelines, before we share our information, we must be ever vigilant about securing sensitive data and sharing that data in a secure environment. But we must also develop reliable and repeatable governance and risk management processes that will foster information sharing.

Lastly, since our world of information technology is evolving more rapidly, additional technologies, such as attribute-based access control, become central to assured information access. With these technologies, we can ensure that consumers of information are authorized access using standards-based identity management solutions.

Ultimately, information sharing is all about the data. We need the ability to find the data, access it, sort through it and combine it to develop information, intelligence and knowledge, and then make those findings available. Some of today's ongoing efforts will provide a solid foundation for data standards and information exchange.

The release of Universal Core version 2.0 (UCore) marks a successful milestone toward achieving interoperability. It is a collective effort across four federal departments to create a core standard of the most common data elements across all possible exchanges.

The National Information Exchange Model (NIEM) leverages the data exchange standards efforts successfully implemented by the Global Justice Information Sharing Initiative. It facilitates timely, secure information sharing across the justice, public safety, emergency and disaster management, intelligence, and homeland security enterprises.

The Maritime Information Exchange Model (MIEM) provides standards that support the tracking of maritime vessels, cargo and people with rich metadata associations to support increased information sharing and will provide the foundation for the MDA data architecture.

All of these efforts are based in Extensible Markup Language which is a platform-independent standard. XML requires minimal work to alter existing and legacy systems or databases and can usually be implemented in a matter of weeks to support net-centric information sharing.

The scope of maritime domain awareness is broad, but it is important that we do not try to "boil the ocean." Rather, an incremental approach to implementation will allow us to achieve quick results and build upon successes or troubleshoot issues as they arise. These incremental results also push the cultural, policy and technical barriers one bit at a time.

While my office has the lead for the interagency effort to develop a comprehensive MDA architecture, there are several commands contributing to this important effort, including OPNAV N3/5 (Information, Plans and Strategy), which has the overall lead for MDA within the Navy. Together we will define and refine the aligned sets of tools used to deliver the right maritime information at the right time to authorized users, whoever they are. Information sharing within the context of MDA presents definite challenges, but we are working together to overcome them.

Interview with Vice Admiral Harry B. Harris Jr.
Deputy Chief of Naval Operations for Communication Networks

Vice Adm. Harry B. Harris Jr.

Vice Admiral Harry B. Harris Jr. is the Deputy Chief of Naval Operations for Communication Networks (OPNAV N6) and the Deputy Department of the Navy Chief Information Officer (Navy).

A Naval Academy graduate and naval flight officer, Vice Adm. Harris was selected for the Navy's Harvard/Tufts Program. He attended the John F. Kennedy School of Government at Harvard University, graduating in 1992 with a Master of Public Administration degree. Selected as an Arthur S. Moreau Scholar, he studied international relations at Oxford and Georgetown universities, earning a Master of Arts in National Security Studies from the latter in 1994. While at Georgetown, he was a Fellow in the School of Foreign Service. He is also an MIT Seminar XXI Fellow.

Vice Adm. Harris has logged 4,400 flight hours, including more than 400 combat hours, in U.S. and foreign maritime patrol and reconnaissance aircraft. He assumed his present duties as OPNAV N6 in June 2008. Previous command tours include: Patrol Squadron (VP) 46, Task Force 57/72 and Joint Task Force Guantanamo.

N6 serves as the principal adviser to the CNO for all communication networks and is matrixed with N2 for ISR and N3/5 for Information Operations (IO) and command and control (C2). As the Navy's CIO, Vice Adm. Harris ensures optimum use of Navy information technology/information management (IT/IM) resources.

N6 includes N6F – Warfare Integration, N60/62 – Programming and Fiscal Management and N61 – Capability Analysis and Assessment. CHIPS spoke with Vice Adm. Harris in January about N6's top priorities.

CHIPS: One of the reasons for the stand up of N6 was to gain better visibility into how IT money is spent across the Navy, reduce legacy networks, and invest in more efficient models like service oriented architecture. Can you talk about progress made in this area?

Vice Adm. Harris: We are making good progress in the area of cost visibility. We are doing that in three different ways, with three different methodologies.

First, there is CARS, an acronym that stands for Cyber Asset Reduction and Security. This is an effort to reduce our legacy networks. One of the biggest hurdles to a secure network environment is legacy networks. We have reduced our number of legacy networks from over 1,000 to less than 500.

We have had success with CARS, but we have a long way to go. We want to get that 500 down to less than 200. This is an area of focus for us. Naval Network Warfare Command in Norfolk is responsible for executing CARS. They have a CARS team whose goal is to get us down below 200 networks by 2010. They are on the right glide scope to do that.

The second initiative we have is an Echelon II Command IT Budget Stewardship Review. You may have known it by its former name, 'Capture the Money.' We are trying to establish total IT cost visibility and accountability. How IT money is spent used to be a mystery. Our goal is to eliminate the mystery and make things transparent.

We want to look at execution budget reviews and identify where the money is being spent and recommend realignment of funding that is not executed in compliance with statutes, directives and guidance. We have done a couple of these so far, and we have had some good success. To date, we have been able to realign $100 million in IT funds across a number of commands. That is significant, that is real money.

The last area we call the ITMC, the IT Management Council. This is an effort to consolidate IT decision-making and governance. The CARS team goes after security, the budget stewardship review process goes after money, and the ITMC goes after centralized decision-making and governance.

The ITMC is chaired by the Vice Chief of Naval Operations and the Department of the Navy Deputy Chief Information Officer (Navy…that's me). It is comprised of executive leadership from each of the OPNAV N-codes as well as Fleet Forces Command; NAVAIR (Naval Air Systems Command); NAVSEA (Naval Sea Systems Command); Navy Installations Command; NAVFAC (Naval Facilities Engineering Command); SPAWAR (Space and Naval Warfare Systems Command); NAVSUP (Naval Supply Systems Command); and Naval Network Warfare Command.

There are also executive advisers and those include the DON CIO, Mr. Robert Carey; Assistant Secretary of the Navy for Research, Development and Acquisition, Mr. Sean Stackley; and the Marine Corps DDCIO, Brig. Gen. George Allen, director, C4/CIO. We feel that the ITMC is working, and it serves as a single senior Navy IT decision forum necessary to help us achieve the NNE, the Naval Networking Environment. We are happy about that in the IT Management Council, and we are using it as a tool to get our arms around governance.

CHIPS: What else do you hope to accomplish in your time as N6?

Vice Adm. Harris: I have already talked about governance, security, our decision superiority, and a move toward the NNE, or the Naval Networking Environment. Our challenge is — how do you deliver decision superiority?

I define that as delivering knowledge, information, intelligence, data and orders, and how you do that virtually, instantaneously against 21st century cyber threats and to the warfighter and back in a fiscally constrained environment.

If we had unlimited resources we could achieve unlimited things. The challenge is to achieve great things with limited resources. In order to do that, we need to achieve a true NNE, or Naval Networking Environment. That's going to take a commitment from everyone, not just the N6, to get it right.

We no longer have the resources to develop or field what I call stovepipe network solutions. Our NNE concept is the right move to get our networks in line and integrated for the future.

While I am the N6, I intend to make a focused effort to bring policy, budget, resources and accountability into alignment to establish an effective enterprise approach into the way we do business and deliver those cyber capabilities that our warfighters on the pointy end say they need to execute their mission.

It is really about the warfighters at the end of the day. That is why we are making this effort to get it right.

CHIPS: The Navy is also hampered by legacy business systems. Does N6 have an interest in replacing these systems with Navy Enterprise Resource Planning?

Vice Adm. Harris: The short answer to that is yes, but I will give you a longer answer. We do have an interest in Navy ERP. I believe that it is a major step toward transformation of our business processes in the Navy. It will lead to a modern standardized and interconnected Navy enterprise operation.

This will give us financial transparency, asset visibility and business process effectiveness and efficiency to support our warfighters. That is what ERP is all about at the end of the day. ERP Release 1.0 provides functionality in financial operations as well as program management, materials management and supply chain management.

We are doing this in phases. We started with NAVAIR in 2007. In October 2008, we instantiated ERP at NAVSUP. Later in 2009, we start ERP with SPAWAR. We do NAVSEA starting in 2010 and Working Capital Fund activities in 2011.

While ERP is tremendous, it is simply a tool, albeit a high-performing one, with a lot of potential. The use of this tool by folks that know what they are doing, and knowledgeable and motivated users, can get us where we want to go.

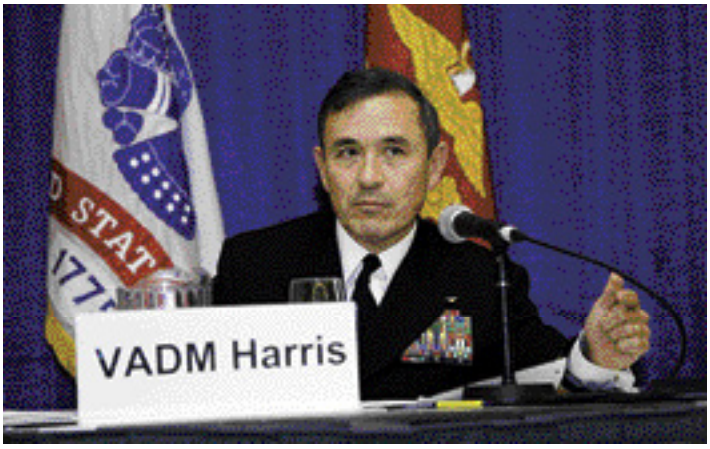
There are two parts, the tool itself, and the people who operate it. They are both equally important.

CHIPS: N6 is directly involved in Next Generation Enterprise Network planning. Can you talk about NGEN?

Vice Adm. Harris: NGEN is part of a larger Department of the Navy effort to create a true net-centric operation across all of our networks. NGEN is the follow-on to the Navy Marine Corps Intranet. With NGEN, we hope to get improved government control and improved flexibility and agility in the way we operate the network.

This is not a criticism of NMCI. NGEN is just the next phase, or level, where we improve and increase our ability to control our own networks. NGEN is going to be the foundation of the NNE. The goal is more adaptability, more reliability and more security to give us more government control and oversight in direct support of the naval warfighter.

N6 and Headquarters Marine Corps C4, along with support from Program Executive Office for Enterprise Information Systems (PEO EIS), Center for Naval Analyses, Naval Network Warfare Command (NETWARCOM) and various other naval organizations, developed the requirements document. N6 serves as the resource sponsor.



OPNAV N6 Vice Adm. Harry B. Harris Jr. speaking in a panel discussion about cyber challenges at West 2009 in San Diego in February. West is cosponsored by AFCEA International and the U.S. Naval Institute. Photo courtesy of AFCEA International.

There is now a separate organization in the Navy called the ACNO for NGEN. That person, the Assistant Chief of Naval Operations for NGEN, leads the System Program Office, the SPO for NGEN. It is a separate office outside N6 on the horizontal line with the other OPNAV N-codes. This brings focus and talent to make NGEN a real thing. CNO has named a two-star admiral to run the SPO, to be the ACNO NGEN, Rear Adm. Bill Goodwin.

CHIPS: Will PEO EIS execute the acquisition?

Vice Adm. Harris: That's a good question. Yes, Rear Adm. 'Grunt' Smith, the new PEO EIS, is responsible for the acquisition.

CHIPS: In 2007, the Secretary of the Navy directed the Navy to demonstrate Maritime Domain Awareness capability in a year. Can you talk about the progress made in MDA technology and doctrine?

Vice Adm. Harris: Maritime Domain Awareness is a big deal. We have accomplished a number of milestones leading up to the present. Just last August we achieved what the Secretary of the Navy directed us to go after — Spiral 1 completion across all the nodes.

The next thing is that the Navy completed a CBA, a capabilities-based assessment, on MDA. The CBA looked at where the Navy's gaps are and how we conduct MDA and offered up a couple of solutions that will allow us to bridge those gaps.

The R3B, the Resources and Requirements Review Board, chaired by N8, approved the findings of the CBA last month. The R3B acknowledged that MDA is more than a material piece — it is people, training, and all of the other parts of the enterprise.

OPNAV N3/5 (Information, Plans and Strategy) has the overall lead for MDA for Navy. N3/5 will be working with the fleet on how we will update our MDA strategy. N6 and N2 are the primary resource sponsors.

CHIPS: The war on terror highlighted the need to provide robust, high-speed data exchanges with coalition forces. Can you discuss improvements made to the Combined Enterprise Regional Information Exchange System–Maritime.

Vice Adm. Harris: CENTRIXS is the core piece that we use to communicate with the coalition. We are pressing ahead to improve the robustness, reliability and speed of how we exchange data with our coalition partners in classified and unclassified domains.

We are using CENTRIX-M, the maritime version/variant, today in a wide range of operations around the world, from antipiracy operations off the Horn of Africa to bilateral missile defense testing operations in the Western Pacific, and opportunities in South America, the U.S. Southern Command area of responsibility.

As N6, we fund the Navy's Pacific Region Network Operations Center, PRNOC, in Hawaii, to expand those contingency capabilities. We are pleased with how we are moving forward with CENTRIXS. CENTRIXS is just one part of the overall puzzle, but it is an important piece as we move to improve our communications with our coalition partners.

CHIPS: With the push to consolidate networks, implement new technologies and communicate globally with allies, partners and nongovernmental organizations, how is the Navy handling the bandwidth requirements which must be increasing?

Vice Adm. Harris: We are using the CBSP, the Commercial Broadband Satellite Program, to increase our bandwidth. In 2007, some folks with a good idea conceived it as our Navy's next generation commercial satellite capability. We needed something to replace the leased Commercial Wideband SATCOM Program and INMARSAT-Bravo.

Compared to INMARSAT, it [CBSP] gives us significant improvements. INMARSAT is in the low kilobyte range, 64 to 128 kilobytes. CBSP provides up to 3 megabytes of data transfer.

Initially, when you put it on some of the small platforms, which desperately need something like this, such as our mine countermeasure ships, frigates and coastal patrol boats, they are going to get about three and a half times what they get now. That is significant. I am jazzed up about CBSP. I think it is a good deal.

CHIPS: Can you talk about Information Operations?

Vice Adm. Harris: Part of my tasking from CNO is to look at IO. As we look at the CNO's guidance for 2009, our ability to achieve decision superiority is essential in operating at all levels of war.

Broadly speaking, in Information Operations, we in N6 are going to focus on three different areas. First, we are working hard to bring high IO capabilities to the warfighter in cyberspace. These things in the Naval Networking Environment that I keep talking about are critical to achieving decision superiority.

In the IO mission area of computer network operations, CNO, and the element of computer network defense, or CND, are essential to protecting Navy networks and operating establishments.

Secondly, our IO portfolio must provide asymmetric capabilities to meet maritime challenges. We are developing strong ties to the BMD, Ballistic Missile Defense, antisubmarine warfare, ASW, and irregular warfare programs. We need to be able to meet adversaries with asymmetric capabilities including electronic warfare and computer network operations.

Lastly, we are working hard on future capabilities. Looking forward is as important as refining and polishing where we are today. So let me talk about CANES, the Navy's Consolidated Afloat Networks and Enterprise Services program. It is essential for what we are trying to do in the NNE.

CANES will reduce our physical IT infrastructure on ships. We want to consolidate afloat network infrastructure and core services for the Navy to better operate with our other forces and our own command and control.

We want to speed effort to catch the current wave of technology. That includes service oriented architectures, enterprise solutions, innovative security approaches and state-of-the-shelf hardware.

At the end of the day, we are going to have four elements of the NNE. NGEN will be the biggest and most visible piece because it will affect everyone in the continental U.S.

We will have CANES interoperable on all of our ships. We will have BLII, Base Level Information Infrastructure, or ONE-NET, our overseas network. Then we will have a few legacy networks that we have excepted from the CARS program. CARS goes from more than 1,000 legacy networks today to less than 500 — and ultimately to less than 200.

The four pillars of the NNE are: CANES; NGEN; BLII ONE-NET and those 'excepted networks.' CANES is the shipboard piece.

CHIPS: What do you mean by excepted networks?

Vice Adm. Harris: Those legacy networks that will not be part of NGEN. Today, we would say that they are not part of NMCI. For example, if you were to e-mail me and put my name in with the Navy dot-mil domain, the @navy.mil is the key that this is an NMCI address in the NMCI domain.

If you are working in the medical profession and you e-mail to someone @bumed.navy.mil, BUMED is a clue that there are other domains. BUMED, Bureau of Medicine and Surgery, is on a different legacy network. It will probably be an excepted legacy network because the BUMED network carries personal data related to medical and health.

We have an obligation to protect those excepted legacy networks against 21st century cyber threats which is why they will be 'excepted legacy' and included into the NNE.

Sharon, let me conclude this interview with an interesting point. We [N6] are only a part of the Navy's IT picture. The NNFE, the Naval NETWAR FORCEnet Enterprise, is an enterprise approach to how we govern IT in the Navy writ large.

There are three cornerstones of that enterprise: the Navy's OPNAV N6 (that's me), the Naval Network Warfare Command in Norfolk, commanded by Vice Adm. Denby Starling, and SPAWAR, commanded by Rear Adm. Michael Bachmann, form the NNFE.

I don't do anything without coordinating with the other two corners of the enterprise. The three corners of the enterprise look at the operational piece, the engineering piece and the financial piece — in other words — what we do, how we do it, and how we pay for it.

It is a team effort; IT is a team sport. We are in this together, and we will move forward together. CHIPS

CARS TASK FORCE SHORTENS ORIGINAL TIMELINE

ADDITIONAL STAFF AND INFRASTRUCTURE REDUCTION PUT CNO TASK FORCE AHEAD OF SCHEDULE

By George D. Bieber

There's an age-old adage: *There's no limit to what you can accomplish if you can get a team to do the work together*, and early results from the Cyber Asset Reduction and Security (CARS) Task Force are proof of this concept.

Since inception in October 2006, the CARS Task Force has keenly kept its sights on:

✓ Improving the Navy's enterprise security posture;

✓ Reducing the Navy's information technology footprint; and

✓ Enforcing enterprise behavior and preparing the way for the Next Generation Enterprise Network (NGEN) and Naval Networking Environment (NNE).

Aggressive efforts, with the fleet; systems commands; personnel and training commands; facilities; higher education commands; and all other major Navy commands, have made significant progress in attaining the Chief of Naval Operations' goals for CARS to reduce the number of Navy legacy networks.

In the last year, the CNO accelerated the timeline for reduction from September 2011 to September 2010 and raised the bar for total network reduction from 51 percent to 90 percent!

Enhancing the Navy's Security Posture

According to Neal Miller, CARS director, CARS is focused on improving the Navy's enterprise security posture. "We are eliminating legacy networks ashore by moving their capabilities into NMCI (Navy Marine Corps Intranet) or ONE-NET," he said.

"We're also taking steps to ensure that all networks allowed to remain outside these networks are just as secure and are efficiently managed following common command and control structures."

Miller added that his team is working to find financial efficiencies and help prepare for NGEN. "This could not be done without the positive support of our mission partners — the NMCI and ONE-NET program leads and the Navy's Echelon II command chief information officers."

One of the first orders of business for CARS was to develop written, repeatable processes; including the first-ever Navy-wide criteria for adjudicating whether a shore-based system or application should be allowed to operate outside the Navy's designated enterprise networks: NMCI, ONE-NET and Integrated Shipboard Network Systems (IT-21).

The CARS team has followed processes, making adjustments and refinements along the way. Together with mission partners, CARS is operating as smoothly as a well-oiled machine to keep this complex mission on track.

To illustrate the scope of this effort, when CARS was initiated, the Navy had nearly 1,200 networks, including NMCI, ONE-NET and afloat networks, which make up just 12 of the 1,200 total networks. But by the end of September 2008 that total had been reduced to about 500, including approximately 150 "excepted" networks, or networks outside the NMCI enclave, which leaves 350 networks to be terminated by September 2010.

By summer 2008, the systematic CARS case development process identified secure enterprise solutions for common applications for more than 230 systems to be migrated into NMCI and ONE-NET. These cases were far enough along in the planning process so that actual migration timelines were established.

CARS and Echelon II CIO representatives then teamed up to create an aggregate network termination schedule for 200 networks during fiscal year 2009.

The CARS team will press on for network shutdown, which will leave approximately 150 networks to be terminated before the mission completion date of September 2010.

The majority of these cases are in the NMCI area of support, and common solutions are being applied overseas to help transition systems into ONE-NET.

It is important to note that approximately half of the Navy's total information technology infrastructure is in place to provide capabilities that are either not supportable in, or not appropriate to be provided by an enterprise network.

Examples include Navy higher education networks at the Naval Academy, War College and Postgraduate School; research, development, test and evaluation (RDT&E) networks operated by the Navy's systems commands; high-speed computing conducted by mainframe computers for Navy oceanographic and meteorological services; and selected tactical and training networks ashore.

> CARS will transform network management into a mature enterprise where sound investments in Navy IT deliver definitive warfighting and business value …

"Through the deliberate CARS process, all excepted networks will be secured behind an approved, centrally-managed information assurance/computer network defense (IA/CND) suite," said Charlie Kiriakou, CARS deputy director and security chief.

"This will ensure that the Navy's entire IT network infrastructure will have well understood and consistent security capabilities, whether it is in NMCI, IT-21, ONE-NET or an excepted network," he said.

Previous CARS investments have accelerated transition to Web-based organizational messaging using the Navy Regional Enterprise Messaging System (NREMS); supported accelerated termination of legacy networks overseas (Guam ONE-NET); and consolidated enterprise applications such as the Federal Logistics Data

(FED LOG) and Standard Procurement System (SPS).

In August 2007, certification and accreditation (C&A) for network operations throughout the Navy streamlined CARS and other Navy workflow by reducing net cycle time in the C&A process.

Rob Mawhinney, Navy's deputy operational designated approval authority (ODAA) and deployment lead for C&A, believes that the process improved risk acceptance decisions by the ODAA through higher quality C&A documents.

"This process is not only a positive direction for CARS," Mawhinney said, "but for commands throughout the Navy as well."

Another way to improve quality and reduce the timeline for completing the C&A process is to deploy a software tool to help automate the workflow and development of required C&A documentation.

CARS initiated and funded an acquisition effort by Program Executive Office Command, Control, Communications, Computers and Intelligence (PEO C4I) to field such a tool, C&A Support Tool, or CAST. CAST automates the C&A process from registration through system decommissioning.

If you use a commercial software application for preparing your income tax return, it's easy to understand the value and time-savings that a similar program can do for the C&A process.

"Classified systems that have not had NMCI seat orders placed are included in the network shutdown list," said Lt. Jessie Castillo, deputy director for the CARS operations division.

"Once a solution is identified and sufficient progress made toward implementation, CARS and the NETWARCOM director of operations may allow re-connection of a legacy network."

In view of the fiscal realities and complexity of the mission, the CARS team has been aggressively working to balance the need for demonstrating tangible results, such as infrastructure reductions, security improvements and savings quickly, with the need to define a comprehensive and executable plan to accomplish its mission on or ahead of schedule.

"We will not rush to failure, nor will we allow ourselves to fall into the trap of over-planning and resultant lack of positive action," said Clifford Bussey, CARS operations officer.

"Prudent operational risk must be accepted while adhering to the need to reduce, consolidate and secure our networks. We also need to track the financial savings when we deliver operating efficiencies to support realignment decisions."

Setting the Stage for NGEN and NNE

One of the greatest challenges facing the Navy's shore IT leaders is reducing costs for operating and maintaining major business and warfighting computer systems without reducing readiness.

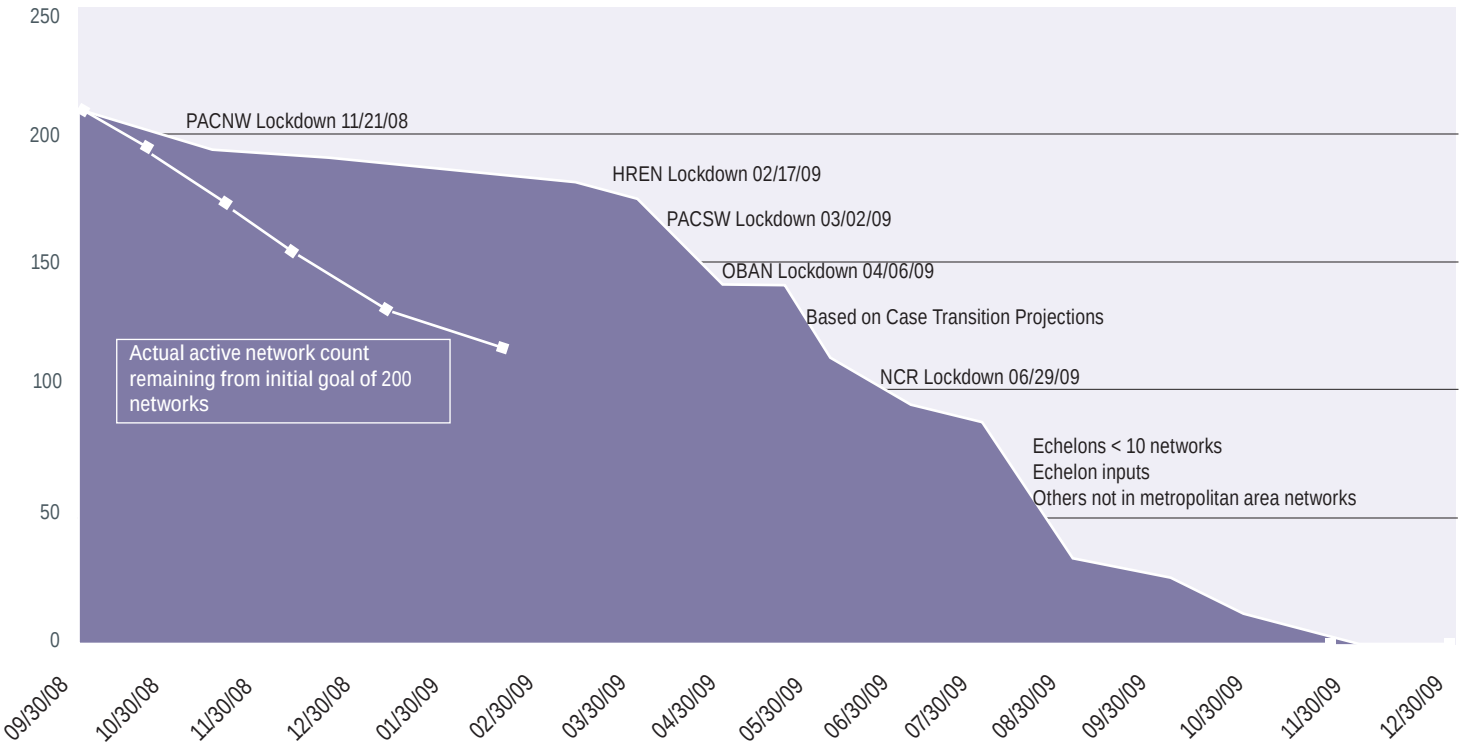
Implementing maturing technologies, such as server virtualization and consolidating systems into fewer physical hosting locations, are key elements of the new Navy Server/Application Hosting Center strategy.

CARS has begun implementation in three locations already, including Space and Naval Warfare (SPAWAR) Systems Center sites in New Orleans and San Diego, and a Bureau of Naval Personnel (BUPERS) site in Millington, Tenn.

The next steps include build out of backup capability for the Millington site at Great Lakes, Ill., and initial exploration for expansion sites in Patuxent River, Md., and Bremerton, Wash.

The strategy includes leveraging joint hosting capacity at large Defense Information Systems Agency (DISA) computing centers. The first one with major Navy users is in Mechanicsburg, Pa., other locations include: Norfolk, Va.; and overseas locations in Naples, Italy; Yokosuka, Japan; and Bahrain. Planned projects are summarized in Figure 1.

Figure 1. Fiscal Year 2009 Targeted Network Projections.



As these sites are activated, many existing Navy systems will be relocated from their current widely dispersed sites into one of the consolidated hosting locations.

In addition to reduced total costs and being more environmentally friendly, the primary benefits of executing this strategy include significant improvements in the Navy's disaster recovery and continuity of operations capabilities; improved ability to defend our key information systems and the data exchanged on them; and an increase in the speed to capability to bring new systems on line securely.

"The overall effort includes seeking most efficient operations as well as identifying appropriate cost-sharing methodology for data centers that host applications owned by more than one Echelon II command," Kiriakou said.

"We will not rush to failure, nor will we allow ourselves to fall into the trap of over-planning and resultant lack of positive action. Prudent operational risk must be accepted while adhering to the need to reduce, consolidate and secure our networks. We also need to track the financial savings when we deliver operating efficiencies to support realignment decisions."

Clifford Bussey
CARS operations officer

"In parallel with consolidating the data centers, Navy is taking positive steps for phased consolidation of our Web portals," Kiriakou added. "These services will eventually be provided via Defense Knowledge Online."

The effort is starting with migration of the U.S. Fleet Forces Command's SharePoint classified and unclassified portals to a DISA computing center in Mechanicsburg. CARS is also implementing consolidation of the Navy's public-facing Web services to a DISA computing center in conjunction with implementation of DoD-level information assurance demilitarized zones, also called proxy services and screened subnets. This is to ensure that the assurance of one system is not undermined by the vulnerabilities of interconnected systems.

"A plan of action and milestones (POA&M) for purging enterprise service capabilities from networks that have attained initial approval as excepted networks will be executed this year," Bussey said.

"I'd especially like to recognize Naval Facilities Engineering Command and the Naval Education and Training Command for timely completion of their POA&Ms, and we are looking forward to helping them execute them to meet all requirements for final approval."

The CARS area of responsibility is global, so CARS has been working hand-in-hand with the ONE-NET program to facilitate enforcement of that network as the Navy's designated enterprise overseas network. This includes coordination of asset and network discovery for overseas networks not presently in ONE-NET and developing engineering plans for them to migrate to ONE-NET.

Supporting Governance

"Another area we are supporting is the emerging governance and architecture plans to enforce a consistent approach for network service types to support the Maritime Headquarters with Maritime Operations Centers," Castillo said.

"Additionally, common themes among the approved excepted networks will be used to ensure full awareness of the potential scope of services required to be provided under the Navy's Next Generation Enterprise Network," he continued.

"Overall, CARS is on schedule," Miller explained. "We have a much better understanding of the detailed scope of networks, applications and systems that will be needed to transition to NGEN, and we are ahead of the game on network terminations.

"We've made great progress with reducing workload for completing security efforts begun under Cyber Condition Zebra with metropolitan area network purifications and security. However, we have not made as much progress as I'd like in a few areas, including establishing Navywide processes and tools for IT asset management," Miller continued.

"Our focus remains on finding a balance between improving security and delivering cost-effective enterprise solutions, but the new normal for security posture, demanded by Joint Task Force–Global Network Operations (JTF-GNO), has driven us to implement a few course corrections to respond to a very dynamic network operations and defense environment across the DoD," Miller said.

Aggressive efforts, with the fleet; systems commands; personnel and training commands; facilities; higher education commands; and all other major Navy commands, have made significant progress in attaining the Chief of Naval Operations' goals for CARS to reduce the number of Navy legacy networks.

He added that, "Active collaboration, with NMCI, ONE-NET and NGEN programs and all the Navy's Echelon IIs, is allowing us to concentrate efforts to meet real-time operational demands to improve our security posture through deploying technologies, such as Host Based Security System and data at rest, while also making real progress to set the stage for NGEN/NNE through initial deployments of IT asset management and Data and Application Hosting Centers."

Miller credited CARS mission partners for the current level of success achieved.

"Together, we will accomplish the CNO's goals, improve [the] Navywide security posture, [and] identify and leverage efficiencies," Miller concluded.

"We will transform Navy IT from a federated to a mature enterprise where sound investments in IT deliver definitive warfighting and business value." CHIPS

George Bieber is the editor of InfoDomain, the professional magazine of Naval Network Warfare Command. This article was reprinted courtesy of NETWARCOM and edited from the original article published in the Winter 2008-2009 edition of Info Domain.

Trident Warrior 2009 Completes Spiral 1 Experimentation

Improving maritime technologies for better security and communications

By Trident Warrior / OLC2 Public Affairs

More than 60 U.S. and coalition personnel participated in the first of a series of experiments at the Navy's newly inaugurated Maritime Operations Center-Experimental (MOC-X) facility on the Norfolk Naval Station, Feb 2-5, 2009. The event was the first of three parts, or Spirals, in the Trident Warrior 2009 / Operational Level Command and Control (TW09 / OLC2) experiment involving critical operational level processes and maritime technologies within maritime headquarters.

The theme of TW09 / OLC2 is building maritime partnerships for regional stability, and the primary goal is to improve maritime security between U.S. and multinational partners.

"TW09 / OLC2 is a great opportunity to bring everyone together in a controlled environment to explore experimental concepts and technologies compatible with warfighter needs," said Capt. Carl Conti, director of Naval Network Warfare Command's Innovation and Experimentation.

"TW09 / OLC2 will leverage the capabilities of a global maritime partnership along with the processes, procedures and emerging tools to reduce uncertainty and speed decision-making," said Capt. Sanford "Sandy" Lansing, director for experimentation, Navy Warfare Development Command. "This will improve maritime security among all the partners."

Spiral One focused on the intelligence preparation of the operational environment. Participants received an initial comprehensive scene-setter briefing with daily intelligence updates based on the current real-world political, military and economic situation throughout the Atlantic, including the Caribbean, North Atlantic, West Africa and Gulf of Guinea, where U.S. and coalition participants currently operate.

The scenario presented problems to challenge warfighters in the areas of maritime situational awareness, information operations, seabasing and logistics, and MOC-to-MOC collaboration requirements and processes.

The coalition MOC participants included Canada, Finland, France, Portugal and the United Kingdom (MOC and NATO Maritime Command Component) and U.S. participants from 2nd Fleet, 4th Fleet, the U.S. Coast Guard and the Office of Naval Intelligence.

"This year's experiment included evaluation of operational processes and procedures along with technical solutions to provide feedback to the fleets," said Capt. Steve Snyder, MOC project team director.

"We continue to look at fleet requirements and solutions involving standardization, examining hybrid warfare, irregular warfare and technologies that will benefit U.S. MOCs, as well as partner nation MOCs," he added. "Aligning with partners and allies is essential in creating globally networked MOCs."

U.S. Navy Cmdr. Patti Enright, 2nd Fleet team lead for developing intelligence preparation for the operational environment, confers with Royal Navy Cmdr. Andy Elvin, MOC-to-MOC Coalition, and Royal Australian Navy Cmdr. Michael C. Doherty, working maritime situational awareness. Elvin and Doherty, foreign exchange officers assigned to Navy Warfare Development Command, participated in the Spiral One experiment. Photo by Mass Communication Specialist 2nd Class Kristopher Wilson.

This experiment was enhanced through the utilization of MOC-X, a state-of-the-art, scalable, flexible and highly adaptable multi-mission venue.

This Navy asset, which achieved initial operational capability in September 2008, is used for operational-level command and control experimentation for the Navy, multinational, interagency, nongovernmental and other governmental agency partners in either a linked or isolated environment.

MOC-X enables the Navy to validate concepts of operations and operational level capability solutions with the ability to address immediate challenges without impacting operational MOCs, emerging missions and/or networks, including procedures, network capabilities and tactical communications.

"During Spiral One, we used a seabasing scenario to conduct initial planning for forward deployed operations at sea and the logistic support necessary for sustained operations. In subsequent phases, we will bring in allied plans and capabilities for mutual support," said Capt. Dorian Jones, operational agent for the Spiral One experiment. The experiment scenario made use of real-world situations with minor modifications to stimulate the interactions we needed to explore."

Coalition partners also had specific objectives for participation in the experiment. Several, including the United Kingdom and Portugal, are looking to improve current collaboration and information sharing in the operational environment.

Finland is using the experiment process as a means to evaluate MOC-to-MOC standard operating procedures. France also participated in the planning process and identified several keys for collaboration to deter drug trafficking, weapons smuggling and terrorist threats.

TW09 / OLC2 is a series of experiments designed to examine technologies and refine, develop, test and explore capabilities to close gaps in the MOC-to-MOC core operational level of command and control.

TW 09 is directed by NETWARCOM and sponsored by Commander, Second Fleet. The Navy Warfare Development Command is supporting the series of OLC2 experiments. CHIPS

For more information contact NETWARCOM public affairs at (757) 417-6706.

Italian Navy Admiral Luciano Zappata
North Atlantic Treaty Organization
Deputy Supreme Allied Commander Transformation


Adm. Luciano Zappata

Adm. Luciano Zappata graduated from Italy's Naval Academy in Livorno, Italy, and was commissioned an ensign in May 1970. The admiral's naval experience is extensive, having served on submarines, destroyers, frigates, and in weapons, combat systems, staff and operational positions.

From 1987 to 1988, he served as commanding officer of the frigate Espero, participating in escort operations to Italian merchant shipping in the Persian Gulf.

From 1992 to 1993, he served as commanding officer of the cruiser Vittorio Veneto, participating in Operation Restore Hope in Somalia and NATO and Western European Union operations in the former Yugoslavia as flagship of the NATO Commander, Standing Naval Force Mediterranean.

Promoted to rear admiral in December 1996, he held the position of Commander of the Second (Blue Water) and Third (Amphibious) Naval Divisions, and CTG 621.01 (Italian Carrier Battlegroup) during Operation Allied Force - Kosovo. He subsequently held various positions, including assistant head of the Navy Development Department, Chief of Staff of Commander in Chief Naval Fleet and Vice Inspector for Naval Logistics Support.

In January 2005, he was promoted to vice admiral and served first as Navy Chief of Staff Advisor and then as Deputy Chief of Staff of the Italian Navy. His most recent tour was Advisor to the Chief of Staff of the Italian Defence.

He was promoted to admiral in June 2007 and assumed the position of Deputy Supreme Allied Commander Transformation July 2, 2007.

ACT is NATO's leading agent for change; enabling, facilitating and advocating continuous improvement of military capabilities to enhance the military interoperability, relevance and effectiveness of the NATO alliance. CHIPS met with Adm. Zappata in February at ACT headquarters in Norfolk, Va., to discuss some of ACT's initiatives and challenges.

CHIPS: What key projects has Allied Command Transformation undertaken recently that may impact maritime security?

Adm. Zappata: In NATO, we have launched in the last year a project called Multiple Futures. We expect this project will support NATO as it begins discussions on what could be the Alliance's next future strategic concept. The existing future concept we have from NATO is a bit old — from 1999. The world has changed and will continue to change. NATO is now involved in operations in Afghanistan. There are many new situations that must be considered.

We were excited at the idea of starting this Multiple Futures Project to understand and to raise the caliber of discussion about the possible future security environment inside NATO and to provide a sound basis for more such discussions at the political and military levels.

This project will influence security discussions and further work within the Alliance and possibly those nations outside of the Alliance. Our aim is to try to influence the definition of the future military challenges — this is how we will be shaping new ideas in NATO. In the Multiple Futures Project, we have identified many drivers of change, from the growth of populations to scarcity of resources and climate change.

For example, if you look at the existing work from the High North (Seminar on Security Prospects in the High North) discussions going on in Iceland, northern countries, like Russia, Denmark, Canada, the United States and all the surrounding countries, we are discovering new innovations because new opportunities, like new sea routes and the possibility of exploiting the bottom of the seas' resources, are opening up.

One of the results we see from this Multiple Futures Project is the importance of the maritime dimension to NATO. Both of NATO's strategic commanders, General James Mattis and General John Craddock, have underscored the importance of the maritime dimension and are working with the nations at the NATO headquarters to agree on a sound way ahead to define a Maritime Strategy and a Maritime Security Operations concept. So far the reactions from the nations are very positive.

CHIPS: What is the focus of NATO's new maritime strategy?

Adm. Zappata: We cannot understand with perfect clarity what the future will hold, but two ideas are important. The first is flexibility. Freedom of the seas when operating in international waters allows you to position your fleets wherever you want at relatively short notice.

You can be present in areas of the world far from your homeports with significant military, political, diplomatic effects. You can cause other nations to be aware of your presence — or not — if you don't want to. You can also establish a limited footprint ashore when needed. That's flexibility. As an example, let's talk about missile defense. You have states with the potential to threaten our countries with missiles. Seas provide freedom of movement for ships and naval platforms, which can operate over the horizon. No one knows that you are there, and you can sail a task force ready to react and be well-prepared.

The Multiple Futures Project team has built an Intellectual Framework that identifies relevant *Drivers* of change that includes several plausible *Futures*. The team has been successful using the framework to focus thinking and improve understanding of how the world may change. From this understanding, we are better able to deduce the strategic-military implications. These implications will be used to develop the best possible military advice for the Alliance and better inform the defense planning processes.

The title of the MFP refers to the future in general, not in military or security terms in particular. The MFP is committed to providing the best possible military advice. But providing advice on military and security matters in the long-term perspective necessitates analyzing the future in broad terms, including the natural, political and social dimensions.

These dimensions combine to shape the various multiple futures the Alliance might face. Each of these futures contains a varied set of security and military challenges from which the team will analyze future security challenges within a broad perspective, using well-known and well-established academic, private sector and military methodologies.

The MFP aims to create the basis for a strategic dialogue within the Alliance – about future challenges, their relative nature and gravity, and how the Alliance should respond to these challenges. The intent with the MFP is not to predict the future of the Alliance; rather the intent is to create a basis for strategic dialogue.

Deputy Supreme Allied Commander Transformation Italian Navy Adm. Luciano Zappata with Executive Assistant Italian Navy Capt. Paolo Pezzutti at ACT headquarters in Norfolk, Va. Feb. 18, 2009.

The second idea is inclusiveness. NATO has discovered the importance of taking a comprehensive approach toward all the other actors at sea. We cannot ignore shipping companies; the International Maritime Organization; nongovernment organizations; and the United Nations.

There are many different non-NATO nations to take into account that are sending their ships to protect their own vessels from piracy. NATO should be more inclusive. We should be able to work with the other actors to find solutions for the future, especially when we share the same challenges and consider the complex international legal framework.

For me, flexibility and inclusiveness are key ideas behind a new maritime strategy.

CHIPS: How does this play into NATO's role with other world organizations such as the UN and European Union?

Adm. Zappata: The United Nations and the European Union are two different organizations. Given the financial problems we are facing and given the globalized world, it is my professional view that if European Union nations want to remain relevant in the future, they must work together. The contributions by individual European Union nations to NATO are significant.

My idea, however, is that the European Union could increase its role and influence within NATO if there were more unity and cooperation among nations. There are many ongoing initiatives in this respect, but there is a long way to go.

The United Nations is a very inclusive organization. That is why it is important for NATO to increase the relationships with the United Nations. I believe we can provide the United Nations with great support.

One of the characteristics of NATO is that NATO is the only existing alliance with a military structure that includes a standing command and control organization. This could be valuable to the United Nations for many reasons, starting for example, with situations where we might provide aid to a disaster or other humanitarian crisis.

This builds trust and confidence in the UN and NATO, while at the same time providing, in some situations, the command and control tools that the UN needs to be effective. It is difficult to do this because there are usually many sensitive political points that may be hard to overcome, but it is a field of opportunity that we have to exploit in the operational community.

"One of the characteristics of NATO is that NATO is the only existing alliance with a military structure that includes a standing command and control organization."

Italian Navy Adm. Luciano Zappata

CHIPS: How has cyber operations challenged NATO's approach to maritime strategy? Is it something you recognize within NATO?

Adm. Zappata: The answer, of course, is yes. Cyber needs to be defined because it is a completely new dimension. Because I am a sailor, I think the characteristics of this dimension are like an ocean. The waves are electromagnetic waves in electromagnetic space. Information technology has given us 'cyber' ships and vessels — a way to use this electromagnetic space — media, radio and TV.

Cyberspace has some very important characteristics. First of all, you move at the speed of light. There is no relevance of space or physical dimensions. You can talk to whoever you want with a simple click or using a cell phone. Distance as a dimension is irrelevant.

The flow of data or amount of data depends only on bandwidth or the dimension of the cyber ship. Cyberspace provides both opportunity and risk for both bad and good guys.

Whenever you sail in this cyber ocean, you can find criminals, pirates and opponents. In cyberspace, the power of nations doesn't matter. You can be the most powerful nation in the world,

and you can be threatened by a few well-prepared hackers. Our enemies are able to exploit weaknesses in this critical field. This is particularly important for the Western countries and for NATO because we rely heavily on information technology. What if our adversaries were able to disrupt this flow of information or break into classified systems?

Of course, we have specific ways of protecting our networks and communications, but it is a continuous challenge. The more we want to use cyberspace to exploit all these opportunities, the more we are at risk of being attacked by others.

Cyberspace is another dimension that the Multiple Futures Project addresses as critically important for its security and military implications. NATO will have to take into account this view.

CHIPS: Can you talk about some other top initiatives for NATO?

Adm. Zappata: Setting aside NATO's operations, such as the International Security Assistance Force in Afghanistan for a moment, I find one of NATO's most future looking actions to be the NATO Training Cooperation Initiative. It was established as a way of sharing allied training expertise with Mediterranean Dialogue (MD) and Istanbul Cooperation Initiative (ICI) partners from the broader Middle East.

To this end, NATO intends to build an expanding network of NATO training activities that will modernize defense structures and train security forces. This initiative is part of the Alliance's continuing transformation of its capabilities and relationships in response to an evermore complex security environment.

I have made many trips to MD/ICI countries, in order to describe to them who we are, what we do, and to exchange our views with them. I have always found these countries very open to improve the reciprocal understanding of culture.

These nations are willing to increase the dialogue and the relationship with NATO, which is essential to build trust and contribute effectively to improve the stability of the area. This initiative from NATO is very important and should be taken up further by the Alliance.

In many situations, like piracy and other maritime issues, we can be inclusive and ask other nations to join us and defend the freedom of the seas, which is in the interest of everybody. The contribution of these countries is vital to be successful.

CHIPS: How is technology used to share information between countries during operations or training exercises?

Adm. Zappata: The exchange of information is the basis of interoperability. Interoperability is a key word because NATO is an organization composed of nations that have different tools and different systems.

Nations want to be free to make the choices they want, and autonomous in deciding what systems or equipment to buy. Interoperability is based on defining and agreeing on a common set of standards or rules and ways of delivering these common services.

It is a continuous circle, in technology and in the real world, things develop day-by-day in communication systems. Interoperability is not something you can buy on the market; it is a process — a continuous effort.

The foundation of interoperability is the will of the nations to be interoperable. There is an organizational aspect of how to achieve and maintain this interoperability. We agree as NATO nations to exchange and share information. That is one of the basic goals. This is where we still have a lot to improve.

While the command and control organization may be a NATO task force, and the commanding officer may be from NATO, it is the NATO nations which provide the forces on the field. Transformation happens in the nations. The nations buy the systems, and they educate and train their soldiers. This is one of the important goals of ACT: to be able to address the nations and give them proper advice.

When I came here, I heard that ACT was the forcing agent for transformation. I did not like the term 'forcing agent' from the beginning because to force you must have authority, you must have tools and a way of enforcing. This cannot work in NATO.

At ACT, we now consider ourselves to be the leading agent for transformation. Leading means having ability [and] good ideas, indicating to nations the way they should move ahead. We can help nations prepare their armed forces for the future while keeping this great value of interoperability.

We have achieved good results with interoperability — especially in our navies. I say that from a personal point of view because of my experiences at sea. We still have to work to improve, especially with the armies, because in the Cold War armies were not expeditionary in nature. This is new for NATO.

In this relationship between the United States and NATO, you are a country well ahead of some European nations in many technological fields, sometimes far more than we conceive.

We need to avoid the risk of the United States going very strongly in some direction with European nations struggling behind. The link here in Norfolk, Va., between U.S. Joint Forces Command and ACT, is valuable for both NATO and the United States. That is why I think that the presence of a NATO command on U.S. soil is important. It says that NATO is more than Europe; it is also the United States and Canada, and we are all together.

It is important to be aware of this because in today's security environment challenges are more globalized, coming from everywhere and affecting all our citizens wherever they are. CHIPS

For more information about NATO Allied Command Transformation, go to www.act.nato.int/.

NATO Training Cooperation Initiative

NATO Training Cooperation Initiative is a way of sharing allied training expertise with Mediterranean Dialogue (MD) and Istanbul Cooperation Initiative (ICI) partners from the broader Middle East. To this end, NATO intends to build an expanding network of NATO training activities that will modernize defense structures and train security forces through an evolutionary and phased approach.

This initiative is part of the Alliance's continuing transformation of its capabilities and relationships in response to an evermore complex security environment. Today, NATO is engaged in operations and missions across three continents ranging from crisis response operations to training missions and disaster and humanitarian relief operations.

In addition, the alliance maintains partnerships, dialogue and cooperation at varying levels of intensity with close to 40 countries, making the family of allies and partners a group that comprises one-third of United Nations member states. NATO is pursuing ever-closer cooperation with other international and nongovernmental organizations, both at the strategic level and in theater.

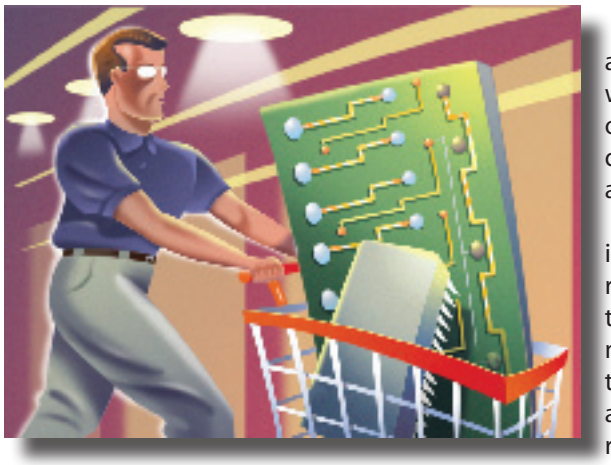
Department of the Navy Launches Strategic Sourcing for IT Equipment

Millions Targeted for Savings on Client and Enterprise Computing

By Floyd Groce and Roger Yee

In this ever-tightening budget environment, the Department of the Navy (DON) has undertaken a strategic sourcing pilot initiative to achieve cost savings and acquisition process improvements.

In 2008, the Assistant Secretary of the Navy for Research, Development and Acquisition (ASN RDA) and the DON Chief Information Officer jointly chartered the DON IT Equipment Commodity Team to achieve the following goals:



- ✓ Reduce total life-cycle costs;
- ✓ Reduce time from requirement identification to delivery;
- ✓ Maximize usage of small business capabilities;
- ✓ Improve the ability to manage IT assets;
- ✓ Increase strategic vendor and IT management;
- ✓ Structure compliance into the acquisition process; and
- ✓ Create a technical foundation for future Naval net-centric operations.

Roger Yee, the Navy's lead for strategic sourcing efforts from ASN RDA, summarized the intended benefits: "Through the DON strategic sourcing initiative, we will not only reduce costs for the department's non-Navy Marine Corps Intranet (NMCI) IT equipment, but will improve our operational efficiency and supply management."

Disciplined Process

To achieve these goals, the team adopted a disciplined and repeatable process (shown in Figure 1) to guide their efforts and align stakeholders' expectations.

"This strategic sourcing process has been proven in numerous projects in the government and commercial sectors yielding significant savings in the acquisition and management of goods and services," said Lido Ramadan from Censeo Consulting Group, a leader in the execution of strategic sourcing in the federal government. "This approach can be applied to many goods or services procured throughout the DON."

As a result of an initial opportunity assessment, non-NMCI IT equipment was identified as the most immediate opportunity to address. This included desktops, laptops, servers, and associated software and peripherals.

Through spend analyses performed in Phase 1 (Profile Commodity), it was revealed that the DON spends more than $500 million on non-NMCI equipment annually. The team learned there were thousands of contracts and a lack of consistent buying guidelines resulting in a variety of equipment configurations, imposing avoidable support and maintenance costs.

With no DON-wide established contracts, along with the disadvantages associated with decentralized and disaggregated buying and funding, the DON's potential negotiating leverage has been greatly reduced.

The Solution

Upon completion of Phase 3 (Develop Commodity Strategy) of the strategic sourcing process, the team developed three vital and integrated strategy recommendations to improve the acquisition of non-NMCI IT equipment. Figure 2 illustrates the three phases of the solution set.

Standards – At the foundation of the strategy is the establishment of DON-wide hardware configuration and buying standards. As part of the stand-up of a Center of Excellence, representatives from various DON networks are analyzing existing configurations and developing DON-wide hardware standards. Standard configurations will help create a technical platform for net-centric warfare, enable better security and information exchange, and reduce total maintenance time and cost.

Contracts – To enable centralized, consolidated purchasing, the DON CIO and ASN RDA joint policy will designate use across the Department of the Navy for the Army's Computer Hardware En-

Figure 1.

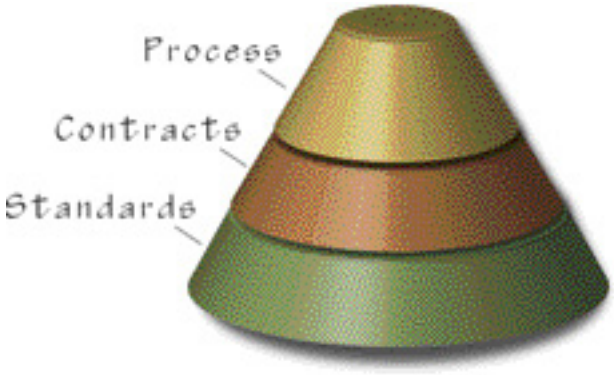


Figure 2. The solution shown in three phases.

terprise Software Solution (CHESS) and the Air Force's IT Commodity Council (ITCC) contracts.

A Memorandum of Understanding is envisioned to formalize the relationship and ensure the availability of DON-specific equipment. For technical requirements that cannot be met through these vehicles, the team will establish new "supplementary" contract(s), which will be open for use across the entire DoD.

Process – To effectively manage the DON-approved buying vehicles, an organization will be designated to manage DON use of the Army CHESS and Air Force ITCC contracts and relationships with these program offices. To consolidate future purchases, a DON-specific process is being developed to aggregate DON IT equipment requirements and funding. Strategic sourcing initiatives often find significant savings from improving how purchases are managed, not only by reducing the negotiated price of a commodity.

Communications

As with any department-wide initiative, communications will be essential for adoption throughout the DON. A formal communications plan will identify DON stakeholders and the best methods of communications and delivery. The team will leverage the Enterprise Software Initiative's (ESI) communications avenues and coordinate future communication efforts through their established channels. DON CIO's application of Lean Six Sigma to ESI will also be leveraged to benefit from DON and DoD-wide enterprise license agreements.

"The DON CIO's Enterprise Software Licensing Lean Six Sigma Project Team has similar findings as the DON IT Equipment Commodity Team," said Floyd Groce, DON CIO team lead for Enterprise IM/IT Planning and co-chair of the DoD Enterprise Software Initiative Working Group. "Both of these projects will benefit as we establish our common DON enterprise processes."

Return on Investment

Considerable savings are expected from the efforts of the DON IT Equipment Commodity Team. This cost avoidance is largely driven by the use of appropriate acquisition vehicles, consolidated purchasing leverage and improved configuration management. CHIPS

DON Enterprise Data at Rest Solution for all non-NMCI Assets is Awarded

The Department of the Navy enterprise solution for protection of sensitive Data at Rest (DAR) on non-Navy Marine Corps Intranet (NMCI) assets is now available. Implementation of this solution enables compliance with Defense Department and DON requirements associated with protection of personally identifiable information (PII) and other types of sensitive DAR on mobile computing devices and portable storage media.

Navy and Marine Corps organizations that need this software should coordinate their requirements through the chain of command to the Deputy Chief of Naval Operations for Communication Networks (N6) and Headquarters Marine Corps (C4) points of contact identified in DON CIO message DTG 312021Z JAN 2009.

On Jan. 23, 2009, the DON awarded MTM Technologies a blanket purchase agreement for purchase of the DON Mobile Armor software bundle. Implementation of this solution enables compliance with DoD and DON DAR protection requirements outlined in Joint Task Force-Global Network Operations Communication Tasking Order 08-009 and DON CIO message DTG 091256Z OCT 07.

All purchases of the DON enterprise DAR solution must be executed through the enterprise agreement, which can be found on the DON IT Umbrella Program's Web site at www.it-umbrella.navy.mil.

Procurement of other DAR protection solutions is prohibited. Organizations that previously acquired or implemented other DAR encryption solutions shall migrate to the DON enterprise solution prior to license renewal.

NMCI successfully piloted its GuardianEdge DAR protection solution in fall 2008 and will be deploying it to all NMCI workstations between March and September 2009. CHIPS

For further information, training and deployment schedules, NMCI users may visit https://www.homeport.navy.mil/management/data-at-rest.

Vice Adm. H. Denby Starling II
Commander, Naval Network Warfare Command


Vice Adm. H. Denby Starling II

Vice Admiral H. Denby Starling II assumed command of Naval Network Warfare Command June 15, 2007. He is responsible for operating, maintaining and defending Navy networks, and conducting information operations, space and fleet intelligence operations.

Overseeing a global force of more than 14,000, he is also the functional Component Commander to U.S. Strategic Command for space, information operations and network operations.

CHIPS spoke with Vice Adm. Starling, with other members of the media, after he participated in a panel discussion about cyber security challenges at a major defense conference in San Diego in February.

Q: In the panel, you spoke about the need for network visibility. I thought the Cyber Asset Reduction and Security and Consolidated Afloat Networks and Enterprise Services projects were addressing the other networks that are not part of the Navy Marine Corps Intranet. What is not visible in the Navy network enterprise?

Vice Adm. Starling: We eventually would like to see as many of the Navy's ships and other networks as possible riding on a single enterprise network. I suspect that we will always have a requirement for some number of networks that are not part of our enterprise system but are protected behind a firewall, for example, research and development networks. Today, the educational networks exist as 'excepted' networks because they have requirements that are, in many cases, fundamentally non-military functions.

Our supply corps will always need to interface with the banking system so their automated teller machines will work. Our hospital networks will always need to electronically interface with other health systems so that healthcare for those in the Navy is seamless.

We contracted with EDS to provide us network services for NMCI. But as the commander at NETWARCOM, I do not have the ability in real time to look into the NMCI network to evaluate its health and whether or not somebody is attacking the network. As we move into the Next Generation Enterprise Network, NGEN will move us from a completely outsourced network to one that the Navy has the ability to exercise a greater level of command and control over and more visibility into.

The percentage of the Navy's networks that are in NMCI today is somewhere near 55 percent. There are large portions of the Navy's networks that are still outside of NMCI, all of our at-sea networks, for example. The Bureau of Medicine and Surgery is outside of NMCI.

CARS has done tremendous work in reducing the number of legacy networks that are out there. The number has gone from 1,200, and we are now in the mid-400s range and hope to get down to 200. As you mature that enterprise network and turn it into a government-controlled network, we'll want to have the tools in place that will give the commander the ability to physically look into the network.

Q: You mentioned Navy excepted networks, aren't they operating under the same Navy security standards?

Vice Adm. Starling: They do, for example, if Company X provides the media for a software tool and they patch it, and they shove out a patch to us across the Navy, we would hand it to NMCI and tell NMCI to push it across all the networks and tell us when they are done.

Then we would pass the patch to all the other guys that own networks, and tell them to put it on their network, and tell us when they are done. They would all report to us when they were done and I would think life is good, but I don't have a way to go in and see if it is really done, I have to depend on what they told me.

We have [network defense and information assurance] systems in the Navy called the Online Compliance Reporting System (OCRS) and the Joint Task Force–Global Network Operations [to protect the Global Information Grid], all the services use these. I then have to go after all the other Navy networks and all the other Echelon II chief information officers and say, do this, and tell me when you have done it.

With NMCI, I only have to tell one 'person,' so I can immediately get the patch out to 55 percent of the Navy's networks. On all the others, I have to wait for them to do it, and tell me they did it. [But] I don't have any way to verify that.

We are deploying Host Based Security System (HBSS) across the Navy. One of the things the HBSS will be able to do for us is to baseline the condition of all the computers in the Navy. As we get this capability fully deployed, it will give us the ability to automate and roll this information up. Then I don't have to depend on somebody telling me that they did it, [instead] all the machines on one layer of the network tell the next layer, tell the next layer, tell the next layer… It all happens automatically.

The bad guys can move quickly. We don't want to have to figure out during the log review, or some other administrative action, that something went wrong. We would like to have better systems to tell us in real time.

Q: Can Navy networks use cloud computing?

Vice Adm. Starling: This is a whole new area for us. From a technical point of view, I am not sure I could give you a well-informed answer right now, but we do have our technical staff looking into it. If you talk to commercial vendors, they have many of the same challenges, like Verizon and AT&T. They operate big networks, and they have real security concerns. Those guys only have to defend the perimeter of where you enter their network.

If I am a customer of Cox Communications at home, and I do a crummy job of keeping my computer patched, I am probably only going to hurt myself. Cox will keep me from doing something stupid that will infect their whole network. In the Navy, I have to care about everybody's computer. If we have a problem, it goes all the

"What we need to understand when we see events like those in Estonia and Georgia is that this is a precursor to the next kinetic fight — or perhaps in place of it. In fact, CNO has stated that the next battle will be in cyberspace and it has already begun. Our President recognizes this and is taking steps to strengthen our national cyber infrastructure."

– Vice Adm. H. Denby Starling II

NETWARCOM Commander Vice Adm. H. Denby Starling II speaking at a panel discussion about the challenges of cyber security at West 2009, cosponsored by AFCEA International and the U.S. Naval Institute in February in San Diego. Photo courtesy of AFCEA International.

the way out to the tactical edge; that makes our world unique.

Even if today I restructured the whole Navy [to take advantage of new technology], I would have to keep the network operating and find the resources to do that. I would have to explain to my leadership why that was important, and what the return on that investment would be. It couldn't be just a performance improvement. It has to be a security improvement. It also has to be a business process improvement.

Q: With NGEN how will you balance accessibility with security?

Vice Adm. Starling: I am security conscious. My job is to guard the gate. Given options, I will normally tend toward the option that is more secure. There are a lot of young people in the Navy who grew up carrying multiple electronic devices. Young Sailors coming into the military today want access. We have to balance that with our requirements for information and network security.

When we first formed our unclassified networks in DoD, these labor-saving devices became great tools with tremendous amounts of capability. Today, we could not live without our unclassified networks. But the unclassified networks are connected directly to the Internet with all the inherent risk.

We have to continue to develop the technology that will allow us to operate in cyberspace where everybody else is and do so in an intelligent fashion so that we can provide an acceptable level of security for the government's unclassified networks.

We have workforce training challenges that any big company has. How do I train the Sailor that just came into the service and is used to clicking whatever he wants to on his home computer or connecting to a P2P (peer-to-peer) server that there are some things you can't do any more?

We do well with that but considering that we have about 700,000 users, if even a small percentage of those don't want to follow the rules you have an opportunity for significant vulnerability. We have to continually address that problem.

We want to be good; we want to be leading edge. Perfect can be the enemy of good enough. We have to ask ourselves what are those essential military functions we want to be able to do. Then we need to buy the technology that will enable us to do them and make sure that those are assured and completely reliable.

The other part of it is that the attack methods change all the time. We have gone from hackers that wanted to take control of your box to the smart guy that doesn't want you to know he was there. We have gone from an era where most of the attacks were phishing to where we see more compromised Web sites and challenges on the Web.

Q: Is NETWARCOM planning mandatory security training for the Navy?

Vice Adm. Starling: We just had a Navywide security focus day to raise the awareness of computer network security for everybody across the Navy. The Chief of Naval Operations directed all Navy activities to conduct a network security training and awareness day no later than Feb. 28. He mandated the training in response to recent security incidents on Navy computer networks.

All Navy commands were given a list of specific training areas and topics, from safe home computing, to phishing, to policy while they are operating Navy computers. NETWARCOM's network security training was Feb. 23 at Naval Amphibious Base Little Creek's theater.

This was not just a one-time initiative. Increased network security must become ingrained in our daily activity on the Navy network. We are trying to tackle a cultural issue.

We often say that the network is a weapons system. In reality, not everybody in the Navy gets to operate a weapons system every single day. While I think that folks who operate at the tactical edge understand this, does the staff officer or the Sailor who works in a staff position? He sees his computer as an e-mail machine or the machine that he does spreadsheet work on, but does he understand that every time he sits down and logs on to that computer, he steps into the exact same battlespace that the bad guys of the world operate in?

I look at computer security the same as force protection, and there is a certain level of awareness that you have to maintain for force protection all the time. After 9/11, everyone's awareness was high. The further away you get from a big event, the level of concern tends to drop off. Once in a while, we need to make it an organizational focus to remind people why this is important.

That is what we wanted to do, remind everybody in the Navy why this is important. All you have to do is open the paper to understand why. It is important to make folks recognize [that] as members of DoD our folks are a target, and they have responsibility to operate their computer in a responsible fashion.

Q: It was reported in the news that embedded chips in card readers that were manufactured overseas were programmed to divert money

from bank accounts. How does outsourcing IT affect our national systems?

Vice Adm. Starling: It is not a surprise to anyone that stuff is being preloaded in commercial software. It is something we have to be aware of. We have committed ourselves across DoD to commercial off-the-shelf solutions; we are going to buy our computers from commercial vendors. The cost to do otherwise would be prohibitive. It is something you have to walk into with your eyes wide open, and it is something you shouldn't kid yourself about.

Since I am probably not going to disassemble and inspect every machine that I ever get and probably wouldn't be clever enough to find everything that might be there even if I did, it becomes all the more important that we continue to develop the tools to help us understand the network's health. Then we can detect anomalous activity on the network and understand what that means as opposed to chasing down everything that is in the box.

Q: Do these concerns that we discussed make conducting electronic warfare and information operations difficult?

Vice Adm. Starling: The ability to do computer network operations: computer network attack, exploit and defend, is dependent on the ability to understand your own network to a very high degree, as well as understanding an adversary's network.

While I provide trained folks who can do the exploit and attack mission, it is not a function that inherently resides within my organization. We have national level organizations that have that responsibility.

We certainly want to have as much knowledge about the adversary's network as I am going to have about my own. Somebody made a good comment earlier [in the panel]: *You can't defend what you can't see.* We will get better at this. It is recognized that we need to do more, but it is a question of what resources you have available to apply to the problem.

Q: We read about the cyber attacks in Latvia/Estonia and Georgia. Are we in better shape than they were?

Vice Adm. Starling: Estonia was an interesting example a few months ago. Estonia, like a lot of countries that have emerged from dark places, was very highly network leveraged. You can deploy networks quickly and because of that they were very vulnerable.

We are certainly dependent on our networks, but I would argue that our networks are more diverse and more highly dispersed. I think that we have more national capability than Estonia did to understand our adversaries and take appropriate steps.

What we need to understand when we see events like those in Estonia and Georgia is that this is a precursor to the next kinetic fight — or perhaps in place of it. In fact, CNO has stated that the next battle will be in cyberspace, and it has already begun. Our President recognizes this and is taking steps to strengthen our national cyber infrastructure. CHIPS

For more information about NETWARCOM, go to www.netwarcom.navy.mil.

Reduce PII Loss by Proper Disposal/ Sanitization of Unclass Equipment

By DON CIO Privacy Team

During the past year, the Department of the Navy has experienced problems relating to turning in excess information technology and office equipment that contain personally identifiable information (PII).

Disposed equipment most commonly found to contain PII includes: office desks, safes, file cabinets, copiers and computer hard drives. Recent audits by the Department of Defense Inspector General and the Naval Audit Service confirm that DON turn-in procedures have not been consistently followed, are inadequate or out-of-date.

While much of the turn-in process involves the Defense Reutilization Marketing Offices (DRMO), Navy Marine Corps Intranet (NMCI) or other DON network owners, the local command or unit is responsible for information security, physical security and property accountability for all excess unclassified equipment awaiting sanitization, shipment to DRMO, or release to another DoD component or donation activity.

The following is a list of lessons learned that should be considered by local commands or units when preparing equipment for disposal.

❑ Use DRMS Instruction 4160.14, dated May 12, 2008, which provides guidance on turn-in of excess equipment to DRMO.
❑ Remove all drawers in desks and file cabinets to ensure stray documents are removed.
❑ Ensure all lockable drawers or cabinets are open for inspection.
❑ Refer to Assistant Secretary of Defense (ASD) Memo "Disposition of Unclassified DoD Computer Hard Drives," dated June 4, 2001, which provides specific instructions on how to dispose of hard drives in the DoD.
❑ Use National Security Agency approved sanitization equipment to properly overwrite and degauss excess unclassified hard drives.
❑ Ensure copier hard drives have been properly overwritten and degaussed.
❑ Develop written policies and procedures to clearly define local command/unit roles and responsibilities.
❑ Provide training for all personnel on how to accurately prepare and process excess unclassified IT equipment before forwarding to DRMO.
❑ Use the Web-based Electronic Turn-in Document (ETID) system for all equipment bound for DRMO.
❑ Ensure verification labels are placed on all hard drives that have been degaussed and overwritten.
❑ Keep accurate destruction and turn-in records for a minimum of five years. CHIPS

Hold Your Breaches!

By Steve Muck

The following is a recently reported compromise of personally identifiable information (PII) involving the transmission of an un-encrypted e-mail which contained National Security Personnel System (NSPS) performance ratings of employees within a Navy region. Incidents such as this will be reported in each subsequent CHIPS magazine to increase PII awareness. Names have been changed or removed, but details are factual and based on reports sent to the DON CIO Privacy Office.

Two non-password-protected attachments to an e-mail were sent to approximately 700 employees. The attachments were created for each NSPS pay pool and provided a bar chart of pay pool results presented as a single Microsoft PowerPoint slide.

A subordinate field activity reported that some of the employees had access to the underlying information that was used to build the slides. The initial investigation showed that, despite command efforts to prevent disclosure, it was possible to manipulate the attachments and reveal privacy sensitive data.

Data included: name; civilian grade; employee identification number, as assigned by the Defense Civilian Personnel Data System (DCPDS); salary; and fiscal year 2008 rating of record for the NSPS employees at the affected command.

No Social Security numbers or other PII was compromised. CHIPS

Steve Muck is the DON CIO privacy team lead.

Lessons Learned

- This incident could have been avoided if proper warnings from the NSPS Program Office about downloading NSPS data to a PowerPoint presentation had been followed.
- While performance rating information does not meet the standard definition of PII, the information in this breach is privacy sensitive and must be treated as such.
- Strict controls must be in place so that only those personnel with a need to know have access to performance rating information.
- The NSPS Program Office has been advised of the compromise of information and will work on a fix to prevent a recurrence.
- All electronic or paper copy documents containing PII must be marked with the following: FOR OFFICIAL USE ONLY - PRIVACY SENSITIVE: Any misuse or unauthorized disclosure of this information may result in both criminal and civil penalties. Refer to: Secretary of the Navy (SECNAV) Instruction 5211.5E.
- Official e-mails containing sensitive information must be digitally signed. Refer to DON CIO message DTG 032009Z OCT 08.
- E-mails containing 25 or more PII records must be encrypted using WinZip or another authorized DON enterprise solution. Refer to DON CIO message DTG 171952Z APR 07.
- Additional privacy information can be found on the DON CIO's Web site: www.doncio.navy.mil.

HOLD YOUR BREACHES! STOP THE LOSS OF PII!

The DON CIO has posters available for download to display in your command. Visit our Web site at www.doncio.navy.mil and search on "posters."

Interview with Rear Admiral John M. Richardson USJFCOM Strategy and Policy Directorate (J5)

Rear Adm. John M. Richardson

Rear Adm. John M. Richardson is the Director of Strategy and Policy (J5) for U.S. Joint Forces Command.

In addition to numerous sea tours aboard the attack submarines USS Parche, USS Salt Lake City and the ballistic missile submarine USS George C. Marshall, the admiral commanded the attack submarine USS Honolulu and Submarine Development Squadron 12, where the six submarines assigned to the squadron made seven extended deployments including six deployments in support of Operation Enduring Freedom.

Ashore, he has served on the staff of the Chief of Naval Operations, Attack Submarine Division, as Naval Aide to the President of the United States, and as the Prospective Commanding Officer Instructor for the Commander of Submarine Forces, U.S. Pacific Fleet.

A 1982 graduate of the U.S. Naval Academy, Richardson also holds master's degrees from MIT and the National War College. He reported to U.S. Joint Forces Command in November 2007.

In December 2008, U.S. Joint Forces Command released a strategy document that forecasts possible threats and opportunities that will challenge the joint force in the future. The report, the 2008 Joint Operating Environment, has been in the forefront of discussion by the media and defense strategists since its release.

JOE 2008 examines trends and disruptions in the geopolitical and military landscape, such as: demographics; globalization; economics; energy; food; water; climate change and natural disasters; pandemics; cyber; and space.

These trends form the framework for exploring the following types of scenarios: competition and cooperation among conventional powers; potential challenges and threats; weak and failing states; the threats of unconventional power; proliferation of weapons of mass destruction; technology; the battle of narratives; and urbanization.

JOE 2008 is meant to be read in conjunction with the Capstone Concept for Joint Operations (CCJO), which was signed by Chairman of the Joint Chiefs of Staff (CJCS) Navy Adm. Mike Mullen Jan. 22, and developed with assistance by USJFCOM. Representatives from the Army, Navy, Air Force, Marine Corps and Coast Guard, as well as U.S. Special Operations Command and U.S. Strategic Command, also assisted in the JOE and CCJO development.

The CCJO describes the chairman's vision for how the joint forces circa 2016-2028 will operate in response to a wide variety of security challenges which are discussed in JOE 2008.

JOE 2008 contributes to USJFCOM's central mission to develop a vision for how our military forces will conduct future operations and tests this vision in the most realistic and challenging ways possible. CHIPS met with Richardson in January to discuss the JOE.

CHIPS: Can you explain what the JOE is?

Rear Adm. Richardson: The nature of the Joint Operating Environment is to provide an operational framework to outline the challenges and opportunities that will face the joint force in the future. Gen. Jim Mattis, USJFCOM's commander, points out in the Foreword that making predictions about the future is always risky.

The JOE does not propose to be any better than past predictions, but the process is important because if you don't do it, you're almost guaranteed to be caught by surprise if you haven't thought your way through the potential challenges.

The Joint Operating Environment document itself may not be as important as the process of getting senior leadership in national security to consider and discuss the possibilities — what are the potential threats and opportunities, and then what are the signposts along the way as we chart our course into the future?

We think it is important to consider not only those things that will change, but also those things that are going to be enduring, particularly with human nature which has been an enduring feature. The fundamental nature of war has been enduring since Thucydides or Sun Tzu wrote thousands of years ago about the nature of conflict and human behavior. Many of those things hold true today.

The nature of war will stay the same, but the character of war will change quite a bit as technology changes and as the enemy adapts. As the strategic environment changes, that will change the character of war.

We look at those trends and how they may potentially affect change on the character of joint force operations, how those trends may combine to form what we call contexts. The contexts we see are a little more robust and complex than individual trends.

Finally, the unique contribution to the Joint Operating Environment is that it focuses on the joint force, and the final step

in the logic is discussing the implications of these trends and contexts on joint force operations of the future.

CHIPS: What I found so compelling about reading the JOE is that in the 21st century, there continues to be profound competition for basic human needs such as food and water. The State Department and U.S. Agency for International Development could do much to help poor countries. Is JFCOM engaged in discussion with these agencies?

Rear Adm. Richardson: The Joint Operating Environment proposes the problem statement. The natural next step is to decide what you are going to do about it and how the joint force is going to operate in response to the environment discussed in the JOE. That response is discussed in the Capstone Concept for Joint Operations.

The Joint Operating Environment document sets the problem, and the Capstone Concept for Joint Operations talks about how the joint force will respond to meet the problems and opportunities that the JOE talks about.

Many of the problems posed in the Joint Operating Environment are going to require solutions that certainly go beyond the military.

Joint Forces Command is closely involved with other branches of our government, other elements of national power — the State Department, the Treasury Department, and the Department of Agriculture for interagency solutions — extending even further into a multinational realm, because we are not going to fight alone; we are not going to face these challenges alone.

[There are] lots of opportunities and Joint Forces Command is looking at the future towards ways we can bring these partnerships together and craft productive solutions.

It may be that in a number of these areas, for instance, in engagement, or reconstruction in response to a crisis, where the military is not in the lead. We may provide support to another government agency or multinational coalition that is much better suited to take the lead.

CHIPS: Who is the audience that you are targeting — the joint force, Congress … Is the JOE intended to convince an audience about the threats? Would the average citizen benefit from reading it?

Rear Adm. Richardson: Our target audience are the leaders and professionals in the national security field. Our approach is if the idea is compelling, it will start the conversation about these ideas. So we hope to provide a compelling case for discussion for some of these potential futures. It is just a perspective.

We tried to make it readable; it is unclassified, and it has gotten plenty of distribution online. It is on our Web page (www.jfcom.mil), and anybody can download it.

CHIPS: The JOE discussed how the power of a few individuals, or single person, can cause global instability. Do you put a lot of weight on the power of one individual to do that?

Rear Adm. Richardson: When we talk about the role of the individual, we come at it in two different ways. We can talk about trends and plot those from point to point and draw a nice curve, but one of the enduring things about the future is that no matter how hard or how diligently we prepare, we are never going to be able to eliminate surprise from our future. We will be surprised.

We have to design a force built to sustain surprise, so we will have the fewest regrets when that surprise comes — not if it comes. In terms of the features of the joint force for the future, that's where the ideas about balance and resiliency and adaptability enter the discussion.

If you take a historical look, one of those areas where you can see surprise come in, where history is fragile, where you can see these disruptions, is in the role of very powerful individual leaders. You can pick them out — both good and bad — throughout history and see that one single individual personally made a tremendous difference. Things could have been very different with a different person in charge — leaders matter a great deal.

Winston Churchill would be a great example of a leader that made an essential difference in the outcome of World War II. On the other hand, if Hitler had not risen to power, we might have seen a much different situation in Germany.

If we talk about discontinuities or potential surprises, who rises to power, how much power they have, and how they use that power, can be hard to predict.

The other place where the JOE talks about individuals is through globalization and the Internet; those forces give a single individual tremendous reach now. You can literally be sitting at your computer and reach out across the world. An individual can have significant effects; we call it a 'super-empowered' individual or 'super-empowered' guerilla.

Another way to look at this is that the cost of entry is very cheap for many disruptive and high-end types of systems. It is literally the cost of a piece of hardware, a computer and an Internet account to launch something with severe effects.

It is becoming affordable to have high-end technology, and if you extrapolate that into the weapons business, you can easily

"… One might also note how much the economic and technological landscapes outside of the military have changed. Economically, in 1983 globalization was in its first stages and largely involved trade among the United States, Europe, and Japan. The tigers of Southeast Asia were emerging, but the rest of the world seemed caught in inescapable poverty. Just to give one example: In 1983, the daily transfer of capital among international markets was approximately $20 billion. Today, it is $1.6 trillion.

"On the technological side, the Internet existed only in the Department of Defense; its economic and communications possibilities and implications were not apparent. Cellular phones did not exist. Personal computers were beginning to come into widespread use, but their reliability was terrible. Microsoft was just emerging from Bill Gates' garage, while Google existed only in the wilder writings of science fiction writers. In other words, the revolution in information and communications technologies, taken for granted today, was largely unimaginable in 1983.

"A revolution had begun, but its implications remained uncertain and unclear. Other advances in science since 1983, such as the completion of the human genome project, nano technologies and robotics, also seemed the provenance of writers of science fiction."

– Extracts from the Joint Operating Environment 2008

"There is always going to be uncertainty [in war], and there is always going to be a human element no matter how many satellites or how much ISR (intelligence, surveillance, reconnaissance) we have. We are never going to be able to know everything." – Rear Adm. John M. Richardson

see that in the not too distant future, a weapon with precision guidance is achievable by anybody who has cash.

It used to be that only a nation-state would have that kind of weapon capability. Now some drug cartels have enough resources that they are building submarines in the jungle. Any cash-rich entity can just as easily turn that kind of cash into other emerging weapons systems, say precision-guided munitions.

CHIPS: In writing the JOE, did you have any current leaders in mind?

Rear Adm. Richardson: This is a historically informed approach. If the future of conflict is going to remain a human endeavor, the best school of human nature is our past. We look at how people faced analogous situations in the past and used those as models and scenarios and vignettes to illustrate how they might face similar situations in the future.

The scope of the document is projected eight to 25 years out. We try not to comment on the present-day situation except as it might be consistent with or the starting point of a trend.

CHIPS: There is a cautionary note repeated in the JOE that states that despite the high-tech advances in weapons and communications systems war remains a human endeavor with the same aspects of fog, friction, mistaken assumptions, uncertainty and unpredictability since human history began. It doesn't appear that advanced technology has made a difference at all.

Rear Adm. Richardson: It is important to have an understanding of the enduring nature of warfare. You can talk about future war, and you can talk about technology-enabled warfare. The character will change. Precision-guided munitions have changed the character of warfare.

But there are still fog, friction and uncertainty. The human elements are not going to change as long as this is a human challenge. It is not a weakness; it is the nature of the problem. There is always going to be uncertainty, and there is always going to be a human element no matter how many satellites or how much ISR (intelligence, surveillance, reconnaissance) we have. We are never going to be able to know everything.

That is why we think it is important to have an appreciation of what is enduring and what will change as technology advances and the strategic landscape shifts. It [war] is human-centric and leader-centric — enabled by technology.

CHIPS: Do you think there can be a game-changing technology development that can change the JOE's presumptions?

Rear Adm. Richardson: One way is that you could have a single disruptive technology that nobody saw coming, a new invention that could have an unanticipated game-changing effect.

Looking back in history, we have also seen that it is not a new technology but some new way to combine tools in a way that we didn't foresee, for example, the radar warning system in Britain [during World War II].

Even though the Germans had better technical radars, it was the operational concept of Britain commanders combining those radars into a network they used as a system that was defining.

The IED (improvised explosive device) is an example of a simple technology used in disruptive and asymmetric ways.

CHIPS: The JOE discusses the effects of globalization and the interconnectiveness of the world economy. It says that countries are very much interdependent and have too much to lose in lives and national treasure to engage in a major war. Will that be a factor in maintaining global stability?

Rear Adm. Richardson: That has always been a factor in whether a nation chooses to go to war. Is the risk worth the gain? Globalization has tied us all together in new ways and accelerated the problem. Now we have tremendous amounts of information and tremendous amounts of capital being transmitted around the world in quantities and speeds that were previously unforeseen.

The processes that control those transactions have to adapt to a much higher bandwidth and a much higher response time. Things can avalanche a lot more quickly.

CHIPS: The JOE discusses the possibility of nations forming anti-American alliances? Do you see this as likely?

Rear Adm. Richardson: It is a possibility. You can almost see the beginnings of it forming. We are naïve if we go into the future thinking that everybody is going to like us. As our enemies connect with each other they are going to find ways to foil our plans and disrupt what we are trying to accomplish. There is the potential for them to link together and form some kind of alliance.

CHIPS: The JOE talked about the rise in the militaries of Russia, China, other Asian countries, and the disarmament of some European countries. Can you talk about how these instabilities and tensions create situations in U.S. military operations?

Rear Adm. Richardson: It comes to that question of balance that we have mentioned a couple of times. That is the ultimate end-state. One of the enduring natures of war is that the enemy is going to focus on your vulnerabilities. He is studying us as much as we are studying him. They are going to try to find out where we are weak, and they are going to direct their attack into that weakness.

Right now, I would say that we are superior in conventional, state-on-state and fleet-against-fleet warfare. Nobody is going to take us on. Up in the blue sky, nobody is going to take us on there.

Where we need to achieve the balance is to maintain that conventional superiority even as we improve so that we are just as superior in irregular, unconventional types of conflict. That is where the importance of intelligence is, in watching what that balance is in the conventional force area so that we don't let the enemy steal the march on us as we are improving our capability in irregular and unconventional war.

"The future operating environment will be characterized by uncertainty, complexity, rapid change, and persistent conflict. … The United States will necessarily be a leader nation to which much of the rest of the world will look for stability and security. It will continue to fall to the United States and its partner nations to protect and sustain the peaceful global system of interdependent networks of trade, finance, information, law and governance.

"…Of the conditions that are changing, perhaps the most significant is what one observer has described as 'The Rise of the Rest' — the increasing ability of other states to challenge the United States for influence, if not globally, then certainly regionally. The economic and military predominance that has underwritten U.S. foreign and defense policy for the past two decades can no longer be assumed."

– Extracts from the Capstone Concept for Joint Operations 2009

Rear Adm. John M. Richardson in his office at JFCOM Jan. 20, 2009.

CHIPS: How would you recommend your colleagues view the JOE?

Rear Adm. Richardson: It is a starting point for discussion. If you want to make practical use of the ideas in the study, you would take the context of the potential futures and use them in your war games, in scenarios for experimentation and for future concept development …

CHIPS: The JOE calls for reform in the acquisition process and personnel systems. Do you have any recommendations?

Rear Adm. Richardson: That is in a specific section of the study called 'Leading Questions.' We have focused this study at the operational level of war. It is not the strategic level, and it is certainly not a policy document. Those two topics are policy matters, but they have operational implications.

If we think about the types of capabilities we need to face the challenges and opportunities in the Joint Operating Environment, just from an acquisition standpoint, it is getting expensive to do business. Some of our competitors have different economic systems.

We use the example of space programs. Compare the cost of our space program to the space program in China. It would be interesting to see how different those are. China is able to put together a capability for a lot less cost.

A lot of people would be in agreement that our system needs to be more responsive. Our enemy is adapting very quickly. He does not have the defense industrial base, the bureaucracy, and all the processes we have to field a new capability. We need to stay up with his adaptation, and beyond that, be able to generate some uncertainty in the enemy — to inflict some difficulty in his thought processes and create some uncertainty about what he thinks about our future. That requires a more responsive acquisition approach.

CHIPS: How? It takes a long time to field major weapons systems.

Rear Adm. Richardson: Being able to field capabilities more quickly and being able to prototype more capabilities so you can keep the enemy guessing about what sort of things you are going to bring to the fight. What sort of things can impose costs on him so that he has to think about spending some of his capital to hedge against these uncertainties. Cost-imposing strategies would be a great goal for acquisition reform.

CHIPS: What about the changes to the personnel system?

Rear Adm. Richardson: [We need to] think about the sorts of skill sets that are required to improve our capabilities and to become superior in some of these human types of warfare. We need to have a better understanding of some of the people we are going to be working with, what their culture is, what their language is, what their motivation is, and what their history is.

We need to think about how our personnel system is geared to train and incentivize the joint force for the future. Do we need a new construct for how we build the joint force?

But again, these are leading questions. The answers will come from changes to policy, but they will have implications on the way we operate the force.

CHIPS: The military is required to do so much more than in the past.

Rear Adm. Richardson: Some of the skills are not traditionally the ones that we have developed. How do we educate those leaders for this new type of fight? The senior enlisted are going to be making important decisions in very complex scenarios. How do we train that person to have the awareness and the tool-set to make an informed decision in that type of environment? That is beyond the scope of the JOE, but we want to pose the problem; the details about potential solutions are the next step.

CHIPS: Is there anything more that you would like to add?

Rear Adm. Richardson: It's important, as we consider the entire document, to understand the context in which we produced it. We are not making any hard predictions, as we said, these are always risky. It is certainly not policy — we went outside the bounds of policy to stretch the range of possibilities for people to think about. It is these possible threats and opportunities, posed in the Joint Operating Environment, that are the starting point for a discussion about national security.

The Capstone Concept for Joint Operations then describes how the joint force will operate in the future to meet the challenges described in the JOE. CHIPS

Web 2.0 in the Federal Government

Entering the age of collaboration

By Brian Burns

There are a few frontiers left to explore: space; the world's oceans; Earth's inner space; microscopic and nano inner spaces; and cyberspace.

Exploration in these areas is led by many federal agencies such as NASA, the National Oceanic and Atmospheric Administration, the National Science Foundation and the departments of Commerce, Defense and Homeland Security.

Each of these frontiers relies on the advanced tools of cyber technology to facilitate exploration. In this article, we will explore cyberspace and discuss the changes that brought us to the use of Web 2.0 in the federal government.

Evolution

Cyber technology cannot be considered in isolation of business needs and missions. It has evolved as a strategic investment to support business needs and missions and has been consistently constrained by computing power; bandwidth; storage; geography and geospace; and security and privacy concerns.

Advances in technology have had a dramatic effect on society causing shifts in cultural models, social structures, economics and living conditions. Humankind has evolved from feudalism to the agrarian age, to the industrial age, to the information age — and now — to the present age of collaboration.

Up until the industrial age, we relied on animals and our brains and brawn to accomplish tasks and make decisions. Through the industrial age we relied on electro-mechanical devices, human analysis and human cognition to make decisions and execute tasks.

During the information age, we relied on computer computation and analysis to execute tasks, and still relied on human cognition to make decisions. During this time, we moved from punch cards and "dumb" terminals, to user interfaces, to ubiquitous interfaces.

We are now poised for ubiquitous computing. Why? Because the cost of memory, bandwidth and storage has rapidly decreased as the capacity of computing power, bandwidth and storage has exponentially increased. Hence, we are now at a point when access to cyber resources is readily available to most of the population.

Grid computing and artificial intelligence (AI) can provide collaborative computing, machine-based analysis, rule-based decisions and execute tasks. Humans are able to tap into both cyber resources and remotely located individuals to accomplish business functions and social activities.

Many baby boomers pioneered cultural change during the information age when they convinced their traditionalist managers

New Web 2.0 tools present a great opportunity to collaborate freely and openly outside the confines of office walls. As artificial intelligence, cloud computing and 3-D imaging evolve, we will immerse ourselves into using our five senses to communicate virtually.

to embrace desktop computing over paper processes to improve business processes and productivity.

Today, Millennials are pioneering cultural change to convince their baby boomer managers to use collaborative Web 2.0 tools, instead of e-mail, time-dependent media broadcasts and structured work hours, to gain process and quality-of-life improvements.

The progression is familiar to many of you. We moved from:

✓ VM (virtual machines) on mainframes to VMware (virtual software) on servers;

✓ Systems Network Architecture (SNA) proprietary priority services to Internet Protocol (IP) standards-based priority services;

✓ 3270 terminals *(display devices used to communicate with mainframes)* to diskless workstations with terminal services — a thin client display window used to view data stored on servers. Advantages of thin client diskless workstations over fat client local disk workstations can include lower production and operational costs, lower power consumption, quieter operation and lowered security risks;

✓ Generalized Markup Language (GML) script to Extensible Markup Language (XML);

✓ Bulletin boards and listservs to wikis;

✓ Automated data processing (ADP), to information systems (IS), to information resources management (IRM), to information technology (IT), to information management (IM), to cloud computing — a style of computing in which real-time scalable resources are provided "as a service" over the Internet to users who need not have knowledge of, expertise in, or control over the technology infrastructure ("in the cloud") that supports them;

✓ Standalone mainframes, to centralized "glass house" or data centers, to networked data centers, to distributed computing, to grid computing, meshed networks and cloud computing.

✓ Mainframe time-shared services to the computing cloud of shared hosts and services.

We used to write letters. Then we talked on phones. Then we wrote e-mails and sent faxes. Next we used cell phones, video conferencing, instant messaging and simple messaging.

Now we use social networking utilities and telepresence, which is a collection of interactive technologies that allow users to interact in real-time with one another from a distance.

We are exploring virtual reality and, in the future, we will use 3-D tele-immersion and other cyber sense technology which will allow users to immerse themselves in another real-time virtual place.

At the end of the day, these media tools fulfill the basic requirement to communicate effectively in what is perceived to be an efficient and cost-effective manner.

Changes in the Federal Government

With these technological advances, the federal government's use of technology to deliver services to citizens and the warfighter is evolving as new technology tools are invented.

At the same time, there needs to be a balance between security and privacy controls and transparent access of government information and services to citizens.

New Web 2.0 tools present a great opportunity to collaborate freely and openly outside the confines of office walls. As artificial intelligence, cloud computing and 3-D imaging evolve, we will immerse ourselves into using our five senses to communicate virtually.

As AI grows evermore intelligent — will it become our sixth sense? As the new cyber frontier opens, we will need to explore it with our eyes wide open; our ears tuned; and our fingers, voice and retinas ready to respond, while abiding by applicable laws and policies.

In government acquisition, Web 2.0 opens the door for more rapid and collaborative responses to requests for information (RFIs), requests for quotes (RFQs), and requests for proposals (RFPs).

Federal procurement specifications will change from the government specifying how contractors are to design and provide systems, to specifying capability and service requirements.

This means that as solutions become global and part of the cloud, industry will need to provide open source and nongovernment-owned, cost-effective solutions that separate the "want to have" requirements from the "need to have" requirements.

The government needs to encourage industry to take a proactive business intelligence and process improvement role and propose alternative ways to approach RFP requirements, if the government does not specify requirements in terms of service.

In the Department of the Navy, the DON Chief Information Officer has encouraged the use of Web 2.0 tools consistent with applicable laws, regulations and policies. (See the DON Web 2.0 article in the CHIPS. January-March 2009 issue at www.chips.navy.mil/archives/09_Jan/web_pages/Web2_0.html.)

Real-time, secure information access by the Navy and Marine Corps is of high interest. Some expectations are that Web 2.0 tools will expand the dimensions of data to allow tagging of the data, not only for content, but for the security level, privacy level, authoritative duration, and authoritative source/location.

As we evolve from the information age to the collaboration age, Web 2.0 tools will emerge as mainstream ways to conduct ongoing business and warfighting.

Change is upon us, and the future is now. CHIPS

Brian Burns is a member of the Senior Executive Service. Mr. Burns is on detail to the DON CIO as deputy CIO for emerging technology from the Department of Education.

FS Tonnerre

Exceptional performance, exceptional crew

By Sharon Anderson

It's difficult to decide which is more impressive— the French command and projection (BPC) ship FS Tonnerre (L9014) — or its crew.

Let's start with the ship, Tonnerre is a marvel of the most modern marine technology and the second ship in its class to be built. The Mistral class launches the French Navy's first all-electric warships.

Construction

Tonnerre, and the first ship in its class, Mistral, are the first military ships to be fitted with a propulsion system using electric PODs, or propulsion orientable drives, supplied by four diesel alternators. Each POD consists of a steerable electric motor housed in a nacelle suspended under the hull. The system, adopted from civilian ship design, consists of two PODs at the stern together with an azimuth bow thruster.

The design allows better maneuverability at low speeds than a fixed propeller and rudder system. Mistral and Tonnerre can make a 180-degree turn in their length and remain stationary in a fixed position. This capability is essential because the Mistral class is a multipurpose ship design that can conduct amphibious operations; evacuation and disaster relief operations; flagship and command and control of a multinational force; and transportation for troops and freight.

Operating under these conditions, the ship can carry out embarkation and disembarkation operations on beaches and in poorly equipped ports.

The demands to reduce costs and construction timelines led to the adoption of a number of innovative solutions, including the simultaneous construction of the bow and stern sections of the Tonnerre on two different sites, with final assembly of the two sections, called "jumboisation" taking place in Brest.

During construction, the French Army and Navy worked closely with the shipbuilders, naval architects and other specialists in a single integrated workplace to promote innovation and to quickly develop joint solutions to problems.

Tonnerre's Commanding Officer Capt. Edmond de Vigouroux d'Arvieu pointed out the ship's unique features during a tour of the ship pierside at Naval Base Norfolk Jan. 28. Tonnerre was in Norfolk to participate in the Bataan Expeditionary Strike Group Composite Training Unit Exercise (COMPTUEX) off the East Coast in February. He was joined by U.S. Navy Capt. Jack L. Sotherland, commodore of the Bataan ESG and commander of Amphibious Squadron Two (PHIBRON 2).

COMPTUEX is noteworthy because Tonnerre and the French antisubmarine frigate La Motte-Piquet conducted joint interoperability training with U.S. Navy and Marine units. "Force projection is Tonnerre's most important mission," d'Arvieu said.

The multipurpose amphibious assault ship USS Bataan (LHD 5) and embarked Marines from the 22nd Marine Expeditionary Unit departed Norfolk Feb. 3 to begin COMPTUEX.

The French captain said Tonnerre's crew is eager to train with their American counterparts, and he enumerated various elements of the ship that are designed to host a multinational task force including a high performance internal and external communications suite which can accommodate up to 200 workstations for a joint/allied headquarters connected to a wide range of radio and satellite communication and information systems.

Thunder

Tonnerre can communicate with anyone anywhere in the world, according to d'Arvieu. A modular plug and play configuration enables multinational forces to connect their own specific equipment to the network that can access any military or civilian network whether French, NATO or European, while offering working conditions similar to those of an inland command post. About 9,600 square-feet of adjustable and prewired partitions can house up to 270 staff officers.

Capt. d'Arvieu explained that the chief advantages of the ship's design are electrical efficiency, better use of ship space and lower maintenance costs. The space gained by the use of the azimuth thrusters means more space for the crew and the construction of cleverly designed compartments that conceal the machinery that runs the ship.

That's the first thing you notice about Tonnerre: the absence of visible pipes, equipment, wires and noise. Despite its name, which translates to "thunder" in English, it's surprisingly quiet on board when compared to the continuous cacophony of machinery operating on most military ships.

Another reason for the unexpected silence is its crew size. Although, Tonnerre can accommodate up to 450 comfortably, its electronic systems significantly reduced the size of the crew traditionally needed to man a ship of its size and multimission functionality. The ship's company includes about 200 officers and crewmembers, according to Lt. j.g. Etienne Gaillard, Tonnerre's public affairs officer.

The second thing you notice about the ship is that its pristine, spacious passageways and compartments make the Tonnerre seem almost empty. But the crew, when you encounter them purposefully rushing about on duty, are smartly dressed with an air of jauntiness that conveys the French Navy's long history which began in the 17th century. The first French Tonnerre, part of the Éclair-class, served from 1759 to 1768. The French Navy, officially the Marine nationale, is often affectionately called La Royale by French citizens.

Multipurpose Design

Tonnerre's designers adopted technology used by cruise ships, according to Gaillard. On a tour of the bridge, he explained a digital surveillance system which monitors the ship's spaces for fire, damage and excessive heat. After he explained the ship's fire control system, Gaillard demonstrated the usefulness of the surveillance system by remotely closing a door on another deck. "As you know, fire is our worst enemy at sea," he said.

Tonnerre is fitted with the latest version

of the combat system used in the French Navy called SENIT 9. The system has an open architecture based on a dual-redundant tactical network interfacing with all weapons and sensors, plus navigation and communications equipment, using protocols including ATM.

A high level of functional integration is achieved in the Combat Information Center (CIC), and bridge operators have access to combat system, navigation, communication and platform management functions. The system also supports other tasks, including mission planning and management, debriefing and on board simulation. The layered software allows all application modules to be independent of combat management system hardware and configuration.

Multi-role radar keeps track of the situation around the ship (air and surface units), and the auto-defense system includes two double short-range Simbad launchers for Mistral missiles, an infrared homing surface-to-air missile.

A new mapping system called SENIN is a significant innovation that enhances water safety and facilitates navigation. But, Gaillard said that the crew also maintains traditional navigational skills referring to a stack of nautical charts within easy reach of crewmembers monitoring electronic consoles on the bridge.

Life Onboard

Located in the forward section of the ship, crew cabins aboard Tonnerre are comparable in comfort levels to passenger cabins aboard Chantiers de l'Atlantique-constructed cruise ships, Gaillard said. Indeed, conveniently fitted with an attractive wood desk and storage unit and stylish carpeting, the cabins are brightly lit and sleek in design.

Officers have individual cabins and hygienic facilities. Senior noncommissioned officers share two-man cabins, while junior crew and embarked troops use four- or six-person cabins fitted with sanitary equipment, which allows the ship to accommodate a mixed crew.

Passageways are peppered with vintage movie posters that recall movies that feature "Tonnerre" or "Thunder" as part of the title, including an old Western from 1960 starring Alan Ladd. In other crew spaces, pretty landscape paintings add a splash of color to the otherwise gray bulkheads.

FS Tonnerre's Commanding Officer Capt. Edmond de Vigouroux d'Arvieu discusses Tonnerre's versatile capabilities during a tour of the ship pierside at Naval Base Norfolk Jan. 28.

Tonnerre

Fact File

The keel for Tonnerre (L 9014) was laid down in August 2003 and launched in July 2005. Tonnerre was commissioned in August 2007. Tonnerre, a force projection and command ship, is comparable to the U.S. Navy's dock landing ships which support amphibious operations.

Characteristics

Length: 200 meters or 656 feet
Beam: 32 meters or 104 feet
Maximum speed: 20 knots
Displacement: 21,500 tons – fully loaded
Draught: 6.50 meters or 21 feet
Range at 15 knots > 11,000 nautical miles
Flight deck area: 1 acre
No. of helicopter landing pads: 6
Propulsion: Electric by means of PODs
Crew: About 200 including officers
Deployment Capacity: Troops: 450 to 700
Vehicles: 60 armored vehicles or a squadron of 13 Leclerc class tanks
Helicopters: 12 NH90 or 16 Tigres

The captain said the ship can easily accommodate 450 army soldiers for long deployments while he pointed out a well-equipped gymnasium and separate recreation area filled with games, a bar, television, and comfy-looking chairs and sofas.

Crew comfort is important because Tonnerre is designed for extended deployments, d'Arvieu explained. The combination of maintenance and repair operations were simplified so BPC ships will be technically available 350 days a year, with an average annual time at sea of 200 days or 5,000 hours.

Noise reduction, attractive living quarters, appealing recreational options, a passenger elevator and good food help relieve the inevitable facts of long deployments: extended working hours, boredom, lack of privacy, cramped spaces and unrelenting noise.

There are 20 crewmembers dedicated to food preparation, serving and clean up staffing five messes, one for each rank category. The crew uses a self-service ramp and officers are served seated.

The 9,000 square-foot fully automated galley is centralized and includes a bakery (think buttery croissants) and separate workstations for preparing meat and vegetables. If needed, the ship can carry enough food for 70 days to feed 700 troops, said Gaillard.

A glimpse into one of the messes revealed shiny stainless steel equipment, and a crewmember dressed in a spotless uniform reminiscent of a traditional French chef including a tall pleated toque.

Tonnerre meets Hazard Analysis and Critical Control Points (HACCP), an international standard that is designed to enhance safety throughout the food chain by preventing, reducing or eliminating potential biological, chemical and physical food hazards.

But meeting HACCP does not come at the expense of food quality or taste. As you would expect, the galley serves traditional French cuisine.

Gaillard explained that BPC ships comply with MARPOL international antipollution standards, and no waste is disposed of at sea. Instead, the trash is sorted, compressed and stored for recycling or disposal. He said that even though military ships are exempt from the MARPOL standard, the French Minister of Defense requested that the French Navy comply with the requirement, and he personally inspected the trash system in a visit to Tonnerre.

Combat Vehicles and Helicopters

Tonnerre has the payload capacity and versatility to carry up to 16 heavy helicopters and one-third of a mechanized regiment, plus two Landing Craft Air Cushion (LCAC) hovercrafts or up to four Landing Craft Units (LCU).

Another configuration would allow the well deck to hold 60 combat vehicles including 13 Leclerc tanks. Troops board the vehicles on two vehicle decks covering more than 3,000 square yards.

The flight deck spans more than an acre and incorporates six helo landing pads, one of which is suitable for the Super Stallion. The U.S. Marines use the Super Stallion for a variety of operations that include delivering supplies and transporting troops and equipment and also for assault missions.

Tonnerre's hangar is also fitted with workshops designed to carry out any type of maintenance on board.

Access to the flight deck is provided by

FS Tonnerre is a multipurpose ship designed to conduct amphibious operations; evacuation and disaster relief operations; flagship and command and control of a multinational force; and transportation for troops and freight. Operating under these conditions, the ship can carry out embarkation and disembarkation operations on beaches and in poorly equipped ports. In these photos crewmembers train for the variety of missions they may be called upon to perform.

two aircraft elevators with a unit capacity of 13 tons. The air installations include a Decca Bridgemaster DRBN-38A approach radar; a Glide Slope Indicator, an instrument landing system for vertical guidance; and a Horizon Reference System.

Medical Services

Tonnerre boasts a modern 8,000 square-foot hospital consisting of 20 rooms, including a dental suite, triage room, radiology room, two operating theaters and a burn treatment center. There are about 70 beds, 19 of which are designed for intensive care. The capacity of the hospital can be increased by an additional 50 beds.

The helicopter hangar can be converted into a field hospital by the deployment of Army Medical Service Technical Equipment Modules to expand services. The hospital is fitted for telemedicine and has a CT scanner.

Routinely, the ship has a medical doctor and two nurses aboard. If needed, modular elements can be added to provide four surgical rooms and accommodate a 100-person medical team, including 12 surgeons.

Sea Trials

Tonnerre was commissioned in August 2007 after a long endurance mission for comprehensive sea trials. Since then the ship has conducted several operational deployments.

The aim is to qualify the ship in various environments, such as cold and warm waters and rough seas, and verify that she meets the requirements to fulfill her missions. The call in Norfolk was scheduled ahead of a tactical training in which her interoperability with the U.S. Marines and their equipment will be verified.

The Bataan ESG is also working to meet training requirements in preparation for its upcoming deployment. COMPTUEX is the second of three at-sea exercises designed to prepare Bataan's crew.

Capt. Sotherland said working with Tonnerre's crew will help prepare the Bataan ESG for future maritime partnerships. "No one nation can do it alone. The success of our maritime strategy depends on continued interaction with the world's navies."

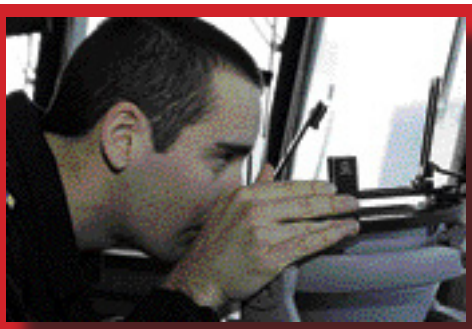
"Honneur, Patrie, Valeur, Discipline"

Even after the impressive tour of Tonnerre, what remains most memorable is Tonnerre's officers and crew, their pride in their ship and their graciousness. During the tour, officers and crew enthusiastically joined the group eager to explain Tonnerre's operations.

French Navy Midshipmen Aurélien de Montgolfier and Fabien Hermant explained flight deck operations. They are students who attend a defense college in Paris run by the French Defense Ministry. As part of their training, they had a choice of deploying with the French Army or Navy and chose the Navy. It is their first time away from home for an extended period. They both said they liked life aboard Tonnerre, they were learning their craft, and the senior officers had taken them under their wing, often using mealtimes to share experiences.

When asked if life aboard the ship lived up to their expectations, without hesitation, Montgolfier said, "It's not what we expect; it's what the [French] Navy expects of us [that matters]." CHIPS

Editor's Note: Thank you to the officers and crew of FS Tonnerre for their cooperation in verifying the accuracy of the facts of this article.



Tonnerre and the antisubmarine frigate La Motte-Piquet joined the Bataan ESG and embarked Marines from 22nd MEU for joint interoperability training in COMPTUEX in February off the Eastern Seaboard. All photos courtesy of the French Navy and French Navy photographers Mathieu LeBresne and Ludovic Picard.

Q&A with U.S. Navy Capt. Jack L. Sotherland

Commodore of the USS Bataan Expeditionary Strike Group and Commander of Amphibious Squadron Two (PHIBRON 2)

French Navy Capt. Edmond de Vigouroux d'Arvieu, commanding officer of FS Tonnerre welcomes U.S. Navy Capt. Jack Sotherland, commodore of the Bataan ESG and commander of PHIBRON 2, aboard Tonnerre pierside at Norfolk Naval Base in preparation for COMPTUEX. Photo courtesy of French Navy photographer Mathieu LeBresne.

The Bataan Expeditionary Strike Group participated in the Composite Training Unit Exercise off the North Carolina Coast in February. The strike group welcomed participation from the French command and projection ship FS Tonnerre (L9014) , as well as the antisubmarine frigate La Motte-Piquet. Tonnerre is of particular interest because of its unique "off-the-shelf" design. Tonnerre is a versatile platform designed to operate far forward and to support action during complex political or military situations. Her innovative capabilities significantly enhance the French, European, NATO and coalition ability to fulfill forward presence requirements.

The exercise, scheduled by Commander, U.S. Second Fleet, was evaluated by a training team led by Commander, Strike Force Training Atlantic. COMPTUEX is important because it is designed to shape the ESG into a cohesive team ready to meet a variety of missions. It's a critical step in the pre-deployment training cycle for a joint task force. This is the first time that Tonnerre and other French units participated and conducted joint interoperability training with U.S. Navy and Marine units.

Large-deck multipurpose amphibians, LHDs, like Bataan and Tonnerre, can embark, transport, deploy, command and fully support all elements of a marine expeditionary unit, or other land units, inserting forces ashore via helicopters, landing craft and amphibious vehicles. They can also be used for disaster relief, transporting medical and humanitarian assistance, and evacuation of civilians in a civil crisis or disaster.

The strike group is comprised of the amphibious assault ship Bataan, amphibious transport dock ship Ponce, amphibious dock landing ship Fort McHenry, guided-missile cruiser Anzio, guided-missile destroyers Porter and James E. Williams; the Los Angeles-class attack submarine Memphis and a Marine Landing Force from the 22nd Marine Expeditionary Unit. The exercise gives Marines, who have been on the ground in Iraq and Afghanistan, a chance to flex their sea legs and train with the gator Navy.

The supply ship Kanawha, frigates Carr, Doyle, Hawes, Kauffman, Nicholas and Simpson; Los Angeles-class attack submarine Boise; and destroyers Carney, Cole and Bulkeley also participated.

CHIPS spoke with Capt. Jack L. Sotherland several days before the start of COMPTUEX. Both Sotherland and Tonnerre's Commanding Officer French Navy Capt. Edmond de Vigouroux d'Arvieu were anticipating great benefits from working together.

Q: Can you talk about what your hopes are for COMPTUEX?

Sotherland: I have been in command since August of last year, and we started working up with the strike units and started liaison with the French Navy at that same time. The goal of COMPTUEX is to certify the Bataan Strike Group to perform the full range of military operations with an eye toward major combat operations and everything that falls within that, for example, humanitarian assistance, disaster relief, and maritime security operations supporting our maritime strategy.

Based on our country's maritime strategy ("A Cooperative Strategy for 21st Century Seapower") that came out a couple of years ago, we work with our coalition partners and other allied and partner nations such as the French and the French Navy. They bring capabilities that we can build on — that interoperability that Capt. d'Arvieu was talking about during his brief. The Tonnerre has very similar capabilities inherent in our own dock landing ships (LSDs).

We do these operations early on so that when we actually deploy, whether it is working in U.S. Africa Command, the 6th Fleet area of responsibility in the Mediterranean, or in the U.S. Central Command AOR, if we come across the Tonnerre or other French ships, our staffs and our crews will be able to talk the same language.

The French Navy, as everybody knows, has been one of our closest allies since our country was formed in the 18th century. We have always had a very close relationship with the French military, the French Navy in particular.

French sailors were able to operate our Landing Craft Air Cushion (LCAC) vessels at an early stage, their well deck

was designed to operate those, as well as our Landing Craft Utilities, the LCUs, which are huge workhorses. Because we have that interoperability, we can bring our platforms over to their ships and vice versa.

The Bataan Strike Group will be the first strike group to deploy with MV-22s, the Marines' variant of the Osprey, as part of their air combat element. That is a significant capability. If we are eventually authorized to land and operate off large French units, it increases our reach and our ability to do our missions.

The French will work with our Marine brethren putting troops ashore and conducting relief missions from the sea. To do that, we use amphibious shipping, which traditionally uses LCACs and LCUs, and then our H-53s (Sea Stallion) and MV-22s, to bring troops to shore.

We also have surface combatants assigned to the strike group. They provide not just protection for units in amphibious ships, they also provide offshore artillery support to the Marines. That's relatively new to be able to integrate that into our operations.

The Bataan ESG is graded with the same criteria as a carrier strike group. We have the same number of ships. The major difference is our striking power is different; instead of an air wing outfitted with tactical strike aircraft, U.S. Marines comprise our striking power, as well as Tomahawk missiles that we employ from our assigned cruiser and destroyers.

This is what we will do: We go out to sea; we embark Marines at Morehead City in North Carolina, and immediately go into various scenarios that will stress the command and control of the strike staff, as well as the 22nd Marine Expeditionary Unit.

We do this with an eye to make sure that we can communicate well with each other, and we can execute the mission when we are called on from the combatant commander.

After we have done an amphibious landing at about the two-week mark, we will put the Marines ashore in an amphibious assault, and then we will concentrate primarily on the blue side of certifications, which runs the gamut of antisubmarine warfare, air defense exercises, maritime interdiction operations, to maritime security operations.

We spread the strike force along the entire Eastern Seaboard from VACAPES (Virginia Capes) all the way down to the Jacksonville, Florida OPAREA (operations area).

That is somewhat unusual, but we have to do that this time of year because the weather in the VACAPES and North Carolina is rather unpredictable, and there is a lot of training that we could not perform safely if we were not able to go into the warmer, and to a degree, calmer waters of Florida. That's where we do a lot of our maritime interdiction operations.

It also gives us a good chance to stress our command and control using satellite links, our voice communications, and other command and control upgrades that we have received in the last couple of years.

The Bataan just got back from her last deployment about a year ago, so it is a relatively quick turn-around. It is our way of supporting maritime strategy and the fleet readiness program that the Chief of Naval Operations has developed.

Q: When is COMPTUEX going to play out?

Sotherland: It takes place the entire month of February. There is a short turnaround after that because COMPTUEX is the Navy's certification for my strike group and most of March is booked with a Marine certification exercise. The Marines tell us where they need to be to perform their mission, and it is my job to get them there safely.

This is not something new, but training with the French has not yet become routine. The last few COMPTUEXs, whether they involved a carrier strike group, or an amphibious group, utilized other allied nations to participate. It is a win-win for everybody.

Regardless of where the Bataan Strike Group goes, we are going to be interoperable, whether it is operating with coalition allies, NATO allies, or other close partners.

Believe it or not, we occasionally can be challenged when communicating with our British allies because sometimes they don't use the same terms or language that we are familiar with.

Coming up with standard phraseology and developing a common operating picture of where we are and how we disseminate contacts and other information across the link and how we will work together is the only way we can get better.

I was at NAVCENT (U.S. Naval Forces Central Command, U.S. 5th Fleet) for

Bataan ESG Commodore and Commander PHIBRON 2 U.S. Navy Capt. Jack Sotherland, FS Tonnerre Commanding Officer French Navy Capt. Edmond de Vigouroux d'Arvieu and U.S. Navy Capt. Brian Goulding from Commander, Strike Force Training Atlantic aboard Tonnerre. At right, a Marine from 22nd MEU prepares for joint interoperability training with Tonnerre's crew. Photos by French Navy photographer Mathieu LeBresne.

18 months before coming here, and I worked closely with the French Navy because they had command of Combined Task Force 150 for a time; CTF 150 has responsibility for millions of square miles of water off the Horn of Africa, the Red Sea and the Gulf of Aden.

Working with all those navies [in CTF 150], allows us to further develop the capacities and capabilities of navies and coast guards that are expanding their reach further seaward, some for the first time.

Q: Can you talk about how you will use the ships in COMPTUEX?

Sotherland: We have six ships in the strike group. All have flight decks, but only the amphibs have well decks. It is this capability that gives a strike group the opportunity to expand our options. And the participation of Tonnerre gives my staff, as well as the 22nd MEU, much greater flexibility.

If I am using the Bataan as a command and control ship doing one part of a noncombatant evacuation mission, now I may be able to move the Bataan closer in and use the Tonnerre as a receiving ship.

We really don't have a lot of excess space on the Bataan. If you come on board during COMPTUEX, there is no room. We have 10 MV-22s, and they bring a lot of maintenance requirements for people, parts and supplies.

If we had to bring a lot of people onboard the Bataan, it would be a tight fit, but having the advantage of another ship, that is almost as large and has more space internally (because she doesn't support as many aircraft,) is an advantage. And remember, we have the usual complement of Marine and Navy helicopters and AV-8B Harriers that share the deck and hangar spaces, totaling 29 aircraft.

I can say now that we have positioned Tonnerre, that we are positioned to augment for medical facilities. Doctors all speak the same language.

If we had 'persons under control' or we had captured pirates, the national rules of engagement that France operates under allow her [Tonnerre] more flexibility to take those pirates, process them and get them to another country.

If I remember correctly, there was a French yacht pirated in 2008. The French overcame the pirates, captured some of them and transported them to Paris [after extradition was granted by Somali authorities] to stand trial.

Their rules allow them to do that; our rules probably would not have allowed that so we take advantage of what the French can do in the strike group.

Part of my staff's responsibility, and every ship's responsibility, is to maintain a matrix of national rules of engagement that tells us what the United States can do, what the British can do, what the Germans can do, and so on.

Over the last five years in COMPTUEX, we have seen a greater interoperability and ability to take advantage of the strengths of each of the participants.

Q: Can you discuss the technology you will use with the French Navy in this exercise?

Sotherland: A lot of it will be command and control. They use a lot of the same link architecture, and we have the ability to digitally talk to one another and display various contacts.

The technology on Tonnerre is highly integrated which allows it to operate with a much smaller crew. That is eye-opening to me and because of that we can probably stress them [French crew] much faster in high-tempo operations. We would probably augment them with additional liaison officers to advise them on what we are doing.

We don't operate with them as part of NATO yet, but in a bilateral operation. That is why we currently only have the French Navy presence for this exercise.

They do not bring any new revolutionary technology. It is just much more automated and not as manpower intensive.

Q: Will you be using the Combined Enter-

The Bataan ESG is made up of amphibious assault ship USS Bataan (LHD 5); amphibious transport dock ship USS Ponce (LPD 15); amphibious dock landing ship USS Fort McHenry (LSD 43); guided-missile cruiser USS Anzio (CG 68); guided-missile destroyers USS Porter (DDG 78) and USS James E. Williams (DDG 95); the Los Angeles class attack submarine USS Memphis (SSN 691) and a Marine Landing Force from the 22nd Marine Expeditionary Unit.

Also participating in COMPTUEX are: USNS Kanawha (T-AO 196), USS Carr (FFG 52), USS Simpson (FFG 56), USS Boise (SSN 764), USS Cole (DDG 67), USS Bulkeley (DDG 84), USS Hawes (FFG 53), USS Kauffman (FFG 59), USS Doyle (FFG 39), USS Carney (DDG 64), USS Nicholas (FFG 47), and FS La Motte-Picquet (D 645) and FS Tonnerre (L9014). COMPTUEX was conducted in February on the Eastern Seaboard.

ATLANTIC OCEAN (Feb. 3, 2009) Capt. Sam Howard, commanding officer of the multipurpose amphibious assault ship USS Bataan (LHD 5) and Capt. Kris Croeber, executive officer, oversee preparations before going to sea. Bataan is conducting composite training unit exercise (COMPTUEX) to prepare for a scheduled deployment later this year. U.S. Navy photo by Mass Communication Specialist 3rd Class Stephen Oleksiak.

ATLANTIC OCEAN (Feb. 18, 2009) Seaman Jack Brown stands aft lookout watch aboard the multipurpose amphibious assault ship USS Bataan (LHD 5). Bataan is participating in a composite training `unit exercise with members of the Bataan Expeditionary Strike Group. U.S. Navy photo by Chief Mass Communication Specialist Tony Sisti.

prise Regional Information Exchange System to communicate with the French Navy?

Sotherland: CENTRIXS is the coalition status quo for us to communicate. Everything that we have needs to go on the CENTRIXS Web site first because if they [French Navy] do not know what our intents are and what we want them to do, then we are not effective. CENTRIXS is the command and control linkage Web server that we will be using.

Q: Can you talk about some of the areas where you hope to learn from the French?

Sotherland: Our Navy has recognized that as Americans we have a tendency to be inward-looking as a culture, and despite the U.S. Navy having been a presence globally for so many decades, I don't think we have done a very good job in the past about learning to adapt to other cultures, but this has been recognized, and there are a number of programs that the Navy is leveraging that will close this culture gap.

One of the most significant efforts is the Center for Language, Regional Expertise and Culture, referred to as CLREC, and I have relied heavily on them to train my staff to better prepare us for our deployment.

It is not just the culture in the Middle East, but in Europe, in the ports of Africa or along the Mediterranean — pulling into Indonesia would be different than pulling into Egypt.

Having cultural sensitivity, knowing the basics of language, how to talk to a different nation, a different people, and not expect them to be like Americans, is one of the biggest things we learn from the French.

In the Indian Ocean, the French have engaged with many countries from a maritime perspective for hundreds of years. If we are going to Dakar or Guinea, I should pick up the phone and talk to my counterpart in the French Navy and ask what he knows about this port and this people, and how not to offend them.

How do I carry our message without seeming arrogant, and how do I limit behavior that could be interpreted as arrogant? What do we usually do when we go to a foreign country? Americans usually talk loud and with our hands and expect to be understood.

Part of my responsibility to my staff, and the ships assigned to me, is to improve cultural awareness, provide rudimentary language training, and find out who speaks the national language within the crew.

I am lucky that a number of members of my staff speak Arabic. We also have some Spanish and some French speakers. We utilize them not just as translators but as cultural points of contact.

I love working with the French, Dutch and Italians, just to name a couple of the far-reaching navies, because they have presence. For instance, the French Navy is everywhere the U.S. Navy is — the Caribbean, Indian Ocean and Pacific. They are very capable, and they have built hundreds of years of interaction with other nations. We can go to our coalition partners, so we do not have to reinvent the wheel.

Q: Do you have a representative from the State Department participating in COMPTUEX?

Sotherland: That is an excellent idea, and we have identified it as a core competency that we should have, but the State Department is still a small organization when compared to the Navy.

We mitigate that with political advisers that are assigned to the various combatant commanders as well as some of their service components. Every one of the staffs that I deal with, whether it is 6th Fleet or 5th Fleet, has a political adviser. They are my points of contact.

NAVCENT also has liaison officers that are stationed in the embassies of many of the countries within the CENTCOM AOR. They are there to facilitate any interaction I have with any nation's military or government.

It works very smoothly. I am looking forward to doing more bilateral and multilateral exercises in support of both the maritime strategy and the various TSCs, or Theater Security Cooperation strategies.

Our overall mission is that we have to be ready to do major combat operations any time and everything else builds on that. Putting Marines ashore in Landing Craft Air Cushions uses the same mechanics as moving civilians on and off the beach for an evacuation.

As we saw with the USS Kearsarge (LHD 3) during Continuing Promise in Haiti after the hurricanes hit, that's a military operation. In that case, we were helping the indigenous people help themselves by providing airlift, manpower, food and supplies.

There were no trigger-pullers — we were not there to take over the country — we were there to help. CHIPS

For more information about the Bataan, go to Navy News at www.navy.mil or contact the public affairs officer at pao@hd5.navy.mil.

INFORMATION ASSURANCE VULNERABILITY COMPLIANCE TRACKING AND REPORTING FOR U.S. NAVY SHIPS

Automating afloat network patch management examinations for fleet IAMs

By Lt. Cmdr. Ricardo Vigil

The protection of Navy shipboard networks is critical to national security. An important part of maintaining a secure network posture is the timely application of software maintenance patches.

In response to this need, the Computer and Network Security Branch at Space and Naval Warfare (SPAWAR) Systems Center Pacific (SSC Pacific) developed the Vulnerability Remediation Asset Manager (VRAM), a new Web portal initiative designed to assist ships in achieving Information Assurance Vulnerability (IAV) compliance.

The tool is used by both the Computer Network Defense-in-Depth Baseline Assessment (CNDIDBA) teams and shipboard personnel to verify shipboard IAV compliancy.

An independent team of Computer Network Defense (CND) experts executes a CNDIDBA during each ship's unit level training phase. The CNDIDBA consists of an IAV compliance scan, a password policy assessment and various security checks on the Common PC Operating System Environment (COMPOSE).

The independent CNDIDBA team performs the IAV compliance portion using the Secure Configuration Compliance Validation Initiative (SCCVI) tool. Each ship must complete a baseline assessment every 24 months or within 60 days following a systems upgrade or major configuration change to the network.

COMPOSE combines commercial off-the-shelf and government off-the-shelf products that deliver directory services, e-mail, Web acceleration, office automation applications, collaboration tools and antivirus software for the Integrated Shipboard Network System (ISNS), Combined Enterprise Regional Information Exchange System (CENTRIXS), Sensitive Compartmented Information (SCI) networks, and Submarine Local Area Network (SubLAN).

COMPOSE delivers these services to the warfighter in a secure software bundle that aligns to the latest Defense Information Systems Agency (DISA) standards and guidelines.

SCCVI is currently employed as eEye Digital Security's Retina© Network Security Scanner; it is DISA's tool of choice for network vulnerability scanning within the Defense Department. Its use is mandated by Navy Cyber Defense Operations Command (NCDOC) Computer Tasking Order (CTO) 06-02. Monthly scans are also conducted by ship's personnel to identify and mitigate network vulnerabilities as they are discovered. This requirement, mandated by NCDOC CTO 06-02, is in response to increased attacks on Navy networks.

To assist the fleet with meeting these monthly requirements, Program Executive Officer for Command, Control, Communications, Computers and Intelligence (PEO C4I), Program Manager Warfare for Tactical Networks (PMW 160) fielded SCCVI on afloat networks.

SCCVI enables the fleet to scan its networks and aggressively track compliance within the IAV Management (IAVM) program. SCCVI provides the ship's information assurance manager an independent analysis of installed IAV patches.

Missing patches identified by SCCVI are downloaded, from SPAWAR's Naval Networks Web site, installed and pushed to the vulnerable machines.

The Naval Networks Web site is the only authorized repository for downloading patches for all PMW 160 programs of record (POR) such as the COMPOSE network systems. Each ship is responsible for achieving 100 percent compliance for all networked systems for which an IAV exists and for which a fix has been released by the respective POR office.

However, a major difficulty with the use of SCCVI is that it does not cross-reference scan results with patches released by the respective POR office. For example, results for a SCCVI scan for COMPOSE would include all missing patches whether or not the patches are approved by the COMPOSE program office.

Until recently, it was the responsibility of either the ship's IAM or the CNDIDBA team to manually parse SCCVI results and determine which IAVs were ship's force fixable or unfixable patches.

Fixable IAVs are patches released by the responsible POR office. Unfixable IAVs are patches that have been identified by the program office but have not yet been released. Ships are not responsible for installing unfixable patches until the responsible program office releases a patch.

To remedy this situation, SSC Pacific launched VRAM, in conjunction with the Fleet Numerical Meteorology and Oceanography Center located in Monterey, Calif., to automate the manual parsing of the SCCVI results as well as establish a repository for the scan data.

VRAM enables the ship's IAM to track

Scan Summaries

Scan Date: TUE FEB 24 22:01:00 UTC 2009
Report: USS NEVERSAIL-SCAN FOR COMPOSE 3.0.x- TUE FEB 24 22:01:00 UTC 2009

Total Number of Hosts Scanned: 88
Total Number of Hosts Fully Patched: 2 (2% hosts fully patched)
Total Number of Patches Available: 182
Total Number of Patches Fully Applied: 152 (83% patches fully applied)

	Fixable	Unfixable	Total
IAVA	14	4	18
IAVB	12	5	17
IAVT	4	4	8

Figure 1. VRAM scan summaries report page.

and monitor compliance with IAVs by removing the labor-intensive manual end-user process of cross-referencing SCCVI scan results with approved patches on the Naval Networks Web site.

To better understand the connection and synergy between SCCVI and VRAM, let us step through a typical vulnerability scan of a shipboard network running COMPOSE.

The ship's IAM would first install and then launch the vulnerability scanner from a workstation that is connected to either the unclassified NIPRNET or classified SIPRNET enclave.

The IAM would then perform a discovery scan of the enclave based on the active subnets to identify all live hosts. The discovery scan results would then be combined into various address groups, defined as a collection of hosts (servers or workstations) related to a specific POR system.

For example, the COMPOSE address group would contain only COMPOSE hosts. Once all of the address groups are created, the next step would be to conduct an IAV audit scan of each group to enumerate a list of vulnerabilities on each system.

For this example, let us continue with the COMPOSE POR. During the IAV audit, the scanner connects to each machine in the address group and compares the machine's installed patches with SCCVI's complete list of IAV patches.

Once the audit is complete, the IAM exports the scan results by generating a Vulnerability Management System (VMS) export file on the completed scan. Instead of manually trudging through the scan results, the IAM can upload the VMS export file to VRAM where it is parsed and automatically cross-referenced with all of the approved patches released by the COMPOSE program office.

Once the VMS file is uploaded, VRAM will output results similar to those shown in Figure 1.

VRAM provides the IAM with a scan summaries report page that contains the following information:

- Total number of hosts scanned;
- Total number of hosts fully patched;
- Total number of patches available;
- Total number of patches fully applied;
- Number of fixable IAV Alerts, Bulletins and Technical Advisories missing; and
- Number of unfixable IAV Alerts, Bulletins and Technical Advisories missing.

The IAM can drill down from the scan summaries report into the remediation report page.

Here the IAM can choose to display the results as follows:

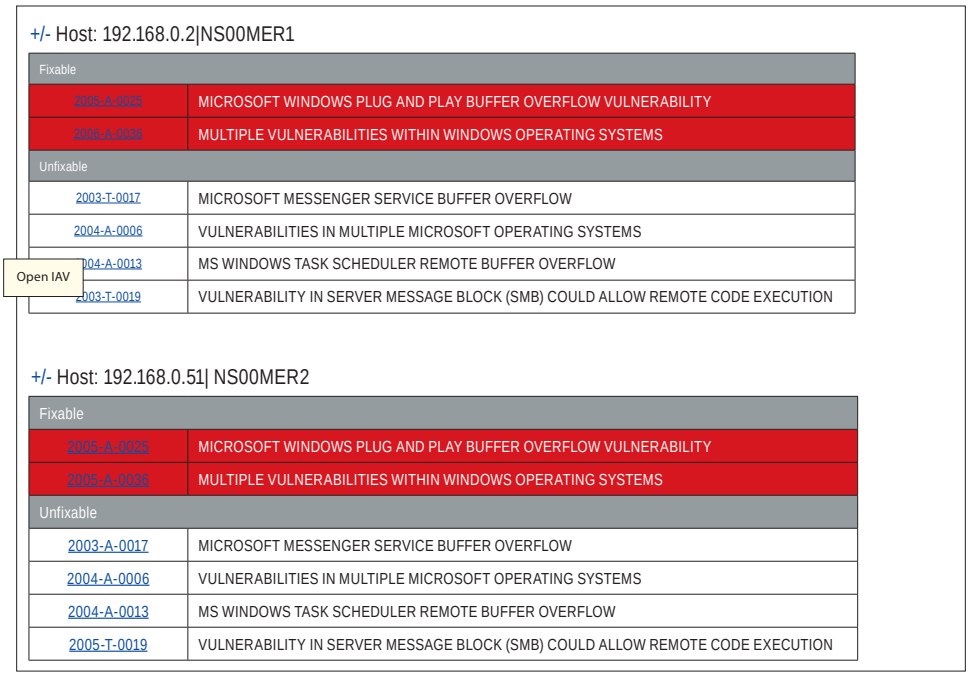


Figure 2. VRAM remediation report page – Vulnerability by Host.

- Vulnerability by Host – displays all available IAV patches missing for each host scanned (illustrated in Figure 2), or
- Hosts by Vulnerability – displays all affected hosts for each available IAV.

The IAM would then use the IAV links on the remediation report page to download the missing fixable patches from the Naval Networks Web site and apply these selected patches to the affected hosts.

The use of VRAM provides a huge improvement for monitoring and fixing network vulnerabilities. Its use not only assists ship IAMs in aggressively managing the IAVM program, but it can also provide Immediate Superior in Command (ISIC), program offices and other computer network defense organizations with visibility into the status of their commands or systems.

There are three types of VRAM accounts:

✓ Site Administrator – the user-based role for a ship IAM; site administrators are able to upload SCCVI scan results and view scan summaries.

✓ Staff Administrator – the user-based role for ISICs or strike group information warfare commanders; staff administrators can create groups of several ships to view the "site posture," i.e., track each unit's IAV compliance trends.

✓ Program Office – the user-based role for the POR office to manage the IAV patch database for its program, view the posture of its cognizant POR systems, or add or associate a unit with a particular POR.

VRAM has proven its usefulness in providing a less labor-intensive means for finding network vulnerabilities, thus improving the CNDIDBA process and expediting remediation actions — as well as freeing ship's personnel to pursue other critical security activities. CHIPS

Lt. Cmdr. Vigil was the Computer Network Defense-in-Depth Baseline Assessment project officer for SSC Pacific. He is currently assigned to Space and Naval Warfare Systems Center Bahrain. Questions regarding VRAM and SCCVI can be directed to ssc_pac_vram@navy.mil. Questions regarding the CNDIDBA evolution can be directed to ssc_pac_cndidba@navy.mil.

INFORMATION ASSURANCE - Taking Commercial Certifications to the Operating Forces

By U.S. Marine Corps Maj. Jeffrey Hammond and Mary Purdy

Because of a 300 percent increase in cyber attacks on Department of Defense (DoD) information technology (IT) systems and infrastructure, there is a critical need for knowledgeable command, control, communications and computer (C4) personnel. To meet this requirement, during 2007 and 2008, Brig. Gen. George Allen, Headquarters Marine Corps, Director C4, identified C4 training as his No. 1 priority to aggressively tackle the cyber domain warfighting mission.

In rapid response, the Marine Corps Training and Education Command (TECOM) not only revamped its Marine Corps Communications-Electronics School (MCCES) classroom training, but also revolutionized the way the Marine Corps trains and now commercially certifies its C4 personnel through Communication Training Centers. The CTCs are collocated with all three Marine Expeditionary Forces (MEF) and provide training for active duty and reserve Marines and civilians who are part of the C4 community, but moreover, for any Marine identified as part of the Information Assurance (IA) Workforce.

DoD Directive 8570.01 mandates that 70 percent of the IA Workforce must be commercially certified by the end of 2009. This creates a high demand for commercial certification training. Specific CTC-developed courses, which respond to the IA mandate, are the CompTIA A+, Network +, Security +, and International Information Systems Security Certification Consortium (ISC)^2 Certified Information System Security Professional (CISSP) certification courses.

In addition to IA certifications, IA technical personnel must hold an operating system (OS) certification. CTC OS courses include the Microsoft IT Academy, Cisco Networking Academy commercial courses, and the Support Wide Area Network (SWAN) Data Incidental Operator Training, which meets the OS requirement with a CTC certificate of accomplishment.

U.S. Marine Corps Maj. Jeff Hammond, the CTC director, invites commanders to reach out to the CTCs located in California, North Carolina and Okinawa for no-cost initial and remedial C4 training. The CTCs have established a relationship with each of the MEFs and through recently signed Memorandums of Agreement have established their role with and in support of their regional area.

The CTCs are equipped to provide both IA and OS commercial certification, but more importantly provide a full commercial certification testing capability for IA workforce personnel. Last year Hammond's staff offered training and certification to more than 840 Marines and civilians. This year he intends to make sure all classroom seats are filled in every hosted class, and therefore, offers standby seats to Navy IA workforce personnel.

The CTCs are designed to relieve the already burdened operating force staffs from the administrative burden of scheduling commercial training and managing seat quotas. Commanders simply request training from their local center and assign Marines to scheduled training. Each CTC, with its respective MEF, co-chairs a quarterly Communication Training Working Group (CTWG) that is designed to identify training requirements, prioritized by need and schedule, to support regional operations and exercise tempo.

At a time when most operating force training focused on equipment-based training in support of the global war on terrorism, the CTC incorporated both fundamental and advanced IA training to enable better security for DoD networks. The CTC staffs are a mix of military, civilian and contractor instructors who are fully trained and certified to teach Microsoft and Cisco Academy courses. This crucial step enabled Marine Corps commands to save several million in training and travel dollars and, instead, focus their efforts on preparation for future deployments.

The CTCs training regimen complements the IA training in MCCES formal classrooms. Both matriculating students, as well as operating force returnees, will have the most up-to-date instruction since using commercially developed training allows quick modifications to the curricula to keep abreast of rapidly changing technology.

For information on CTC class dates and to request training, go to the CTC homepage at: https://www.29palms.usmc.mil/ctc/. Select "Training Schedules" to see class dates or "Warfighter Training Request Portal" to schedule a class.

DON IM/IT Excellence Award presented by DON CIO Mr. Rob Carey and Deputy Director C4/CIO U.S. Marine Corps Mr. Jim Craft to Capt. Russell Cromley, MCCES; and Maj. Jeffrey Hammond, CTC.

Goal 6 of the Department of the Navy Information Management and Information Technology Strategic Plan, Fiscal Year 2008-2009, states: "Develop an agile and integrated IM and IT total force capable of implementing, operating, and managing the power of the NET." Both the formal schoolhouse and the CTC curricula advance this goal and ensure that Marine Corps personnel are prepared to meet the cyber domain demands of current and emerging technologies.

At the DON IM/IT Conference, DON CIO Robert J. Carey recognized the CTC and MCCES staffs for their quick execution of training support to the cyber security mission requirement. Mr. Carey praised TECOM for successfully executing high tempo training requirements while managing limited resources.

Commercial certification training is integral to the DON IA Workforce Improvement Program implementation. Kudos to all involved in establishing this training program as a "best practice." CHIPS

Maj. Hammond is the Director of the Marine Corps Communication Training Centers. Mary Purdy provides contract support to the DON CIO IT Workforce Team.

GOING MOBILE

What's Your Wi-Q?

By Tom Kidd, Department of the Navy, Director of Strategic Spectrum and Wireless Policy

The Going Mobile series of articles began in the January – March 2009 issue of CHIPS. In it we discussed "Enterprise Mobility 2008," the report released by the Department of the Navy Chief Information Officer that describes the process the DON would use to leverage the advantages that commercially available wireless technologies can deliver.

In discussing enterprise mobility during our DON Wireless Working Group session at the DON Information Management/Information Technology (IM/IT) Conference in February held in San Diego, we decided to take a poll to see just how much we personally use wireless technologies. Most of us had never thought of the number of wireless devices we encounter every day.

Using the list at right, take a moment to determine your "Wi-Q" number. Give yourself a point for every wireless device from the list and any others not on the list that you use. You might be surprised.

Please e-mail your Wi-Q number and the names of your wireless devices not on the list to donwirelessteam.fct@navy.mil. CHIPS

Tom Kidd is the Department of the Navy director of Strategic Spectrum and Wireless Policy. In addition to "Going Mobile," he also authors the CHIPS continuing series "Can You Hear Me Now?" which focuses on bringing the complex and often esoteric issues of electromagnetic spectrum to the broader DON community. For more information about the DON Wireless Working Group, contact the DON Wireless Team at donwirelessteam.fct@navy.mil.

Wireless Devices You Use

- ❑ GPS Child Locator
- ❑ RFID Smartcards
- ❑ Contactless Payment Systems
- ❑ Vehicle Data Recorder
- ❑ Wireless Printer
- ❑ Wireless Shower Radio
- ❑ Wireless Bathroom Scale
- ❑ Digital Picture Frame
- ❑ Remote Control Power Outlet
- ❑ Wireless Internet Radio
- ❑ WiFi, Other
- ❑ Wireless Tire Pressure Sensor
- ❑ Garage Door Opener
- ❑ Wireless Motion Hunting Decoys
- ❑ Wireless Remote Trolling Motor
- ❑ Family Radio Service Radio
- ❑ Citizen Band Radio
- ❑ RFID Credit Cards
- ❑ Wireless PDA Keyboard
- ❑ Anything Bluetooth
- ❑ Wireless Cell Phone Headset
- ❑ RFID Key Fob
- ❑ Wireless Security Camera
- ❑ Wireless Weather Station
- ❑ Wireless Light Switch
- ❑ Wireless Thermometer
- ❑ Golf Range Finder
- ❑ GPS Navigation System
- ❑ Automatic Vehicle Location
- ❑ Pet Identification Chip
- ❑ Motion Sensor Lighting
- ❑ Electronic Dog Collar
- ❑ Wireless Dog Fence
- ❑ Marine Radio
- ❑ NOAA Radio
- ❑ Radio Frequency Security Tag
- ❑ Cell Phone Signal Booster
- ❑ Cell Phone
- ❑ Baby Monitor
- ❑ Walkie-Talkie
- ❑ Radio Controlled Airplane
- ❑ Hands Free Cellular Device
- ❑ Wireless MP3 Player
- ❑ Keyless Remote Entry
- ❑ In Bumper Back-up Sensor
- ❑ Wireless 3rd Brake Light
- ❑ Anything WiMax
- ❑ Wireless Recreational Vehicle Levels
- ❑ Atomic Clock Receiver
- ❑ Wireless Workout Monitor
- ❑ Wireless Video Glasses
- ❑ Radar Speed Gun
- ❑ Wireless Tape Measure
- ❑ Motion Sensor Alarm
- ❑ Wireless BBQ Thermometer
- ❑ Wireless Stock Market Reporter
- ❑ Wireless Doorbell
- ❑ Wireless Driveway Alarm
- ❑ Wireless Backup Camera
- ❑ Wireless Network Router
- ❑ Wireless Headphones
- ❑ Wireless USB Network Adapter
- ❑ Anything ZigBee
- ❑ Television
- ❑ AM/FM/HD/Satellite radio
- ❑ Wireless Game Controllers
- ❑ Wireless Speakers
- ❑ Wireless VoIP Phone
- ❑ Cordless Phone
- ❑ Wireless Music System
- ❑ Wireless Internet Video Camera
- ❑ TV Remote Control
- ❑ Wireless Notebook Computer
- ❑ Wireless Gaming Receiver
- ❑ Wireless Computer Mouse
- ❑ Wireless Computer Keyboard
- ❑ Wireless Microphone
- ❑ Wireless Guitar Adapter
- ❑ Amateur Radio (Ham)
- ❑ Personal Emergency Locator Beacon

You Scored...
0-30: You probably own a cassette deck | 31-40: You probably have a Facebook page
41-60: Your spouse thinks you need therapy | 61-80+: You're a Super Geek and proud of it!!

Information Technology Training on NKO

By Chris Kelsall

In March 2009, the Naval Education and Training Command completed changes to the Navy e-Learning site to provide Department of the Navy Information Technology Management Series (2210) personnel the ability to identify and participate in online training supporting their occupations and associated competencies.

Although developed for the IT Specialist 2210 community, learning also supports government civilians and military personnel desiring additional training in IT areas ranging from systems administration to enterprise architecture. The site also provides access to professional development courses that support leadership and interpersonal skills.

To learn more about the training available and to view occupational groups, competency and course mapping, access Navy e-Learning via Navy Knowledge Online (https://www.nko.navy.mil) and click on the Printable Listing link under the Content tab on the left side of the page, then scroll down and click on the DON IT 2210 Competencies Matrix Spreadsheet.

The spreadsheet provides a means to link to course descriptions based on IT 2210 parenthetical titles (2210 IT Job Series Matrix) and Competencies (SkillSoft Learning Asset Map).

Specific directions for accessing, enrolling and completing courses are found under the course access instructions page in the same matrix. Note that only government employees can access these pages.

The development of DON IT and network training is governed by federal law, Defense Department and DON doctrine and policy, and service-specific policy implementing higher level direction.

Today's processes have resulted in what some have called "silos of excellence" where acquisition programs determine requirements for their network, system or application, and the formal schoolhouse training requirements are based upon the capabilities of deployed technology.

To ensure that the abilities of the DON IT workforce progress to support the network environment of the future, training requirements determination, development and delivery must be managed at the enterprise level.

Additionally, how the DON IT workforce accomplishes its tasks and how the services, coalition partners and non-federal agencies do business is changing. The future is filled with new means of collaboration, such as wikis, collaborative Web sites; mashups, which combine and integrate data from multiple sources; podcasts, which provide digital media files distributed over the Internet; and social networking, which was popularized by MySpace and Facebook, and is now being used within the Defense Department and intelligence community to provide a collaborative forum to share information, allow open networking and provide a repository of knowledge.

Today's IT training consists of foundational courses, required information assurance training and certification, factory-delivered training and formalized training programs. The ever-changing roles of government civilians, the infusion of new technologies and the evolving cyber realm require DON personnel to have the ability to rapidly access educational opportunities.

The deployment of this training is one of the steps the DON Chief Information Officer is taking with Navy, Marine Corps and private sector partners to provide the DON IT workforce with opportunities for personal development.

SkillSoft offers a wide variety of online learning designed to meet the training needs of Navy personnel. This includes more than 3,000 self-paced courses covering topics such as business professional, IT desktop and other IT professional skills.

These courses feature strong visual design, a focus on instructional objectives at the application and analysis levels; learner interactivity; reinforcement through role playing and case studies and the transfer of learning into practice through online job aids; follow-on activities; and quick reference guides.

A testament to the quality of SkillSoft content is the recognition these courses have achieved from several accredited colleges as well as professional certification programs.

SkillSoft offers a wide variety of online learning designed to meet the training needs of Navy personnel in the 2210 job series.

SkillSoft courses have been approved to offer continuing professional education credit by programs such as Project Management Institute's Project Management Professional (PMP) certification, the National Association of State Boards of Accountancy and the Human Resource (HR) Certification Institute.

In addition, SkillSoft offers more than 1,000 courses and 60 preparatory exams designed to help prepare an individual for the more than 100 IT certifications that SkillSoft content supports today.

The DON CIO applauds the efforts of the personnel from the Naval Education and Training Command and SkillSoft who made this extensive training possible.

Enrollment and completion of courses identified through this effort, while targeted at the IT 2210 community, are open to all DON government civilian and military personnel.

Comments and recommendations are welcomed and appreciated. Comments may be submitted via the DON CIO Web site by selecting the IT Workforce Topic area at www.doncio.navy.mil/AskAnExpert.aspx. CHIPS

Access Navy e-Learning via Navy Knowledge Online: https://www.nko.navy.mil

Chris Kelsall is the DON IT Workforce team lead.

DON IM/IT Conference, Once Again a Huge Success

Conference provides opportunities for learning and networking with colleagues

By Holly Quick

With more than 900 people in attendance, the Department of the Navy (DON) Information Management/ Information Technology (IM/IT) Conference had something to offer everyone, from the program manager with questions about naval architecture to the contract specialist buying software. The conference offered a venue to share information about the latest DON IM/IT initiatives, policy and guidance, from senior leadership level, to the project lead, to the average IT user.

Hosted by the DON Chief Information Officer, the conference was held Feb. 10-13, 2009, at the San Diego Convention Center. Topics were chosen based on feedback received from attendees of past DON IM/IT Conferences.

Subject matter experts from the DON CIO led 43 informative sessions, which fell under 12 requested topics, including: DON Application and Database Management System (DADMS) and DoD IT Portfolio Repository (DITPR)-DON; privacy; enterprise architecture; Enterprise Software Initiative; DON IT Umbrella Program of contracts; IM/IT workforce; Joint Information Environment; knowledge management; and spectrum/wireless and telecommunications.

It would be impossible to describe all the conference highlights, but one of the most popular sessions featured a town hall meeting with DON CIO Robert J. Carey.

Because the DON CIO is the Community Leader for the DON IT workforce, there were many opportunities for DON IT personnel to engage with DON CIO IT workforce team members. In one session, Chris Kelsall and Jennifer Harper led a spirited discussion with lively participation from the audience on current and future DON IT workforce efforts.

Kelsall summarized the challenges that confront DON IM/IT personnel and described how the DON CIO is taking remedial action. The challenges include:

• Developing a fighting strategy for all areas of cyber and IT;

• The varying call of public service from generation to generation and from person to person;

• Public law placing significant requirements on federal IT employees;

• Maintaining and operating state-of-the-art and legacy systems concurrently;

• Training and educating the DON IT workforce to prepare for the "Pearl Harbors" of cyber;

• Meeting the challenge of helping to ensure that a sufficient talent pool is available for DON IT work; and

• Addressing the challenges of appealing to a diverse multigenerational workforce.

The DON IT Community Town Hall featured guest speaker and former NASA astronaut, Dr. Sally Ride, the first American woman to orbit the Earth.

Mr. Carey and Dr. Ride spoke to a packed house, including San Diego area students. The students were symbolic of the discussion which centered on encouraging students to pursue degrees in math and science and promoting multicultural diversity in the Naval workforce by recruiting talented women and individuals from diverse cultural backgrounds into government service.

Mr. Carey and Dr. Ride talked about the importance of nurturing student interest in the sciences at a young age, especially girls and minorities.

According to Ride, while both girls and boys exhibit about the same amount of interest in science at a young age, interest for girls and minority students diminishes over time. The loss of interest is not due to poor grades or lack of ability, said Ride. The reasons are societal: cultural images of scientists and how they should look and act, and students' fear of not being able to succeed in difficult career fields.

Dr. Ride said there are many ways to reverse this trend, including mentoring students at a young age and encouraging them that careers in the sciences are challenging, rewarding and even patriotic, citing her own reasons for pursuing a degree in physics at Stanford University and choosing to enter the astronaut program.

"The goal of the DON is to be an employer of choice," Mr. Carey said. "The DON strives to offer challenging careers in IM and IT to both civilian employees and military members."

According to Carey, the DON has about 11,000 IM/IT workforce members, not including contractors. He said the workforce is expected to grow within the next five years due to the implementation of the Next Generation Enterprise Network. Open and continuous recruitment will be needed to staff positions required for NGEN governance and security, Carey explained.

The DON CIO is working closely with human resources specialists on innovative recruiting plans which will be designed to attract a diverse pool of applicants. Announcements will be posted on USAJobs (www.usajobs.gov) and the DON's Civilian Human Resources Web site (https://www.donhr.navy.mil) beginning summer 2009, Carey said.

Mr. Carey also discussed some workforce documents being developed: the DON IT Workforce Strategic Plan; the charter establishing an Information Assurance Workforce Management Oversight and Compliance Council; Cyberspace Workforce Policy and Guidance; and Civilian IT Career Paths.

The IT workforce can hear from and engage with Mr. Carey on a regular basis through his podcasts and blogs which are published on the DON CIO Web site.

When an audience member asked Dr. Ride what advice she would give young students, she said, "Reach for the stars. You can be anything you want to be."

To view a full list of the conference presentations and request copies, go to the DON CIO Web site at www.doncio.navy.mil. CHIPS

Don't miss the East Coast DON IM/IT Conference, May 11-14, 2009, at the Virginia Beach Convention Center, Virginia Beach, Va. The conference will be held at the same time and location as the Joint Warfighting Conference 2009, sponsored by AFCEA International and the U.S. Naval Institute in coordination with U.S. Joint Forces Command.

You can register for the East Coast DON IM/IT conference by going to the DON CIO Web site: www.doncio.navy.mil.

2009 DON IM/IT Award Winners Announced

Three individuals and five project teams were honored at the DON Information Management/Information Technology Conference in San Diego for their outstanding contributions toward transforming the Navy and Marine Corps through information technology.

The following individuals and teams were recognized during an awards ceremony, Feb. 11, 2009, by Robert Carey, DON Chief Information Officer; Jim Craft, Deputy Director, C4, Headquarters Marine Corps; Kevin Cooley, director, Information Technology and Information Resources Management, N61; and Vice Adm. H. Denby Starling II, commander, Naval Network Warfare Command.

William G. Reynolds, Naval Education and Training Professional Development and Technology Center CIO/N6 director Executive Management Framework. While serving as NETPDTC CIO/N6, Reynolds created and implemented an Execution Management Framework (EMF) that drove major positive cultural change in a Navy IT organization of 300 employees, which delivers business value to more than 40,000 Sailors annually.

Through his leadership, NETPDTC N6 is becoming a leading entrepreneurial IT organization. Managers now work to define goals, manage customer expectations, and shape increased business value expectations. EMF's resounding success is due to Reynolds' risk taking and challenging his staff to understand and implement transformational change.

Capt. Roy S. Petty, commanding officer, Navy Cyber Defense Operations Command. Capt. Petty is a recognized subject matter expert and leader in the evolving mission area of computer network defense. He fosters a command environment that maximizes the ingenuity and productivity of his cyber workforce.

Under his leadership, the Navy Cyber Defense Operations Command has attained unprecedented levels of success and set a new standard of excellence for all Department of Defense computer network defense service providers.

Lt. Bobby Carmickle, combat systems officer and electronics material officer, USS Freedom (LCS 1). While serving as electronics material officer in the first Littoral Combat Ship, USS Freedom, Carmickle distinguished himself through exceptional performance in the design and implementation of a new and unique Littoral Combat Ship Distance Support architecture.

With a core crew of just 40 Sailors, this unique warship requires a radical new approach to off-ship support. Lt. Carmickle brought this issue to the attention of his chain of command and then led efforts to develop the operational and technical architectures needed to provide the requisite reach-back to support tactical employment of USS Freedom.

Navy Exchange Service Command Payment Card Industry Compliance Project Team for exemplary execution of measures to meet the PCI Data Security Standards compliance requirements. The success of this project resulted in the protection of customers' personal credit card information; preserved the security and integrity of NEXCOM's IT systems, networks and critical infrastructure from compromise; and protected NEXCOM's profits and the associated Navy Morale, Welfare and Recreation (MWR) profit distribution by avoiding the costs associated with fees and penalties for noncompliance.

Headquarters U.S. Pacific Command J6 Portal for significant achievement and leadership in the implementation of classified and unclassified portals at HQUSPACOM. The team set the standard for information dissemination and collaboration in the Asia Pacific region. More than 1,500 users PACOM-wide have enhanced capabilities in the portal environment for warfighting and humanitarian/disaster relief functions, improving decision making.

As a result of the team's efforts, USPACOM is better able to respond to world events and dynamically collaborate with international mission partners.

DON teams and individuals of all ranks, rates and grades are eligible to apply for the annual DON IM/IT Awards. Awards are presented to those who meet one or more of the following criteria: superior leadership skills, delivering results that ensure the organization is working toward common solutions that align to the DON IM/IT strategic vision; innovative use of IM/IT to reduce systems and applications; innovative use of IM/IT to significantly improve the efficiency and effectiveness of the organization in delivering its mission while not duplicating existing projects, systems or solutions; sharing and managing information and knowledge to enable effective decision-making, increase the efficiency and improve mission effectiveness; significant contributions that enable information assurance, computer network defense, critical infrastructure protection and identity management improvements; significant contributions to the recruitment, retention and training of the IM/IT workforce.

For more information about the DON IM/IT Awards, go to the DON CIO Web site at www.doncio.navy.mil.

NETWARCOM Commander Vice Adm. H. Denby Starling with Certification and Accreditation Lean Six Sigma Project members and DON CIO Robert J. Carey.

of the Navy Award Winners

ON through innovative information technology projects

U.S. Marine Corps Information Assurance Workforce Improvement Plan, under the direction of Maj. Jeffrey L. Hammond and Capt. Russell B. Cromley, for revolutionizing the way the Marine Corps trains and now commercially certifies its information technology personnel.

With a 300 percent increase in cyber attacks on Department of Defense IT infrastructure, there is a critical need for knowledgeable IT personnel. The leadership and focused efforts of Maj. Hammond and Capt. Cromley ensure that the Marine Corps is prepared to meet the demands of current and emerging technologies of the cyber domain.

Naval Network Warfare Command Led Certification and Accreditation Lean Six Sigma Project for work that resulted in the successful implementation of improvements in the Navy's information assurance certification and accreditation process.

Using Lean Six Sigma techniques, the team worked with representatives from across the Navy's IT community to overhaul the Navy's process for managing the implementation of information assurance capabilities and services.

The new process that the team developed has been successful in reducing the time it takes to complete certification and accreditation activities while improving the quality and visibility of accreditation decisions.

Navy-Marine Corps Mobilization Processing System for its rapid design, development and implementation of the core system for what has become the U.S. Navy's authoritative Web-based Individual Augmentation tracking system in support of the global war on terrorism.

The development team, comprised of representatives from several key Navy organizations and small business application software firms, used commercial development tools to create a Web-enabled personnel requirements and fulfillment system which operates across DoD secure and non-secure environments using role-based permissions to allow use by commands throughout the world. CHIPS

DON Fed 100 Award Winners Announced

Congratulations to the DON's 2009 Federal 100 award winners. The Federal 100 award recognizes individuals in government and industry who made significant contributions to the federal information technology community in 2008. The awards are presented by the 1105 Government Information Group and Federal Computer Week. The winners were honored at a gala March 25. The award winners are listed below.

Byron Adams – Legal Counsel to the Department of the Navy Chief Information Officer

Rear Adm. Mike Brown – Acting Assistant Secretary for Cybersecurity and Communications for the Department of Homeland Security

Joseph Camacho – Program Director, U.S. Joint Forces Command Joint Knowledge Development and Distribution Capability

Robert J. Carey – DON CIO

Richard Etter – DON CIO Information Assurance and Critical Infrastructure Protection Team Lead

Dan Green – Data Strategy Technical Process Owner, Space and Naval Warfare Systems Command

Barb Hoffman – DON CIO Director of Operations and Director of Investment and Performance Management

Lt. Col. Richard Leino – S-5 Engineering, Marine Corps Network Operations and Security Center

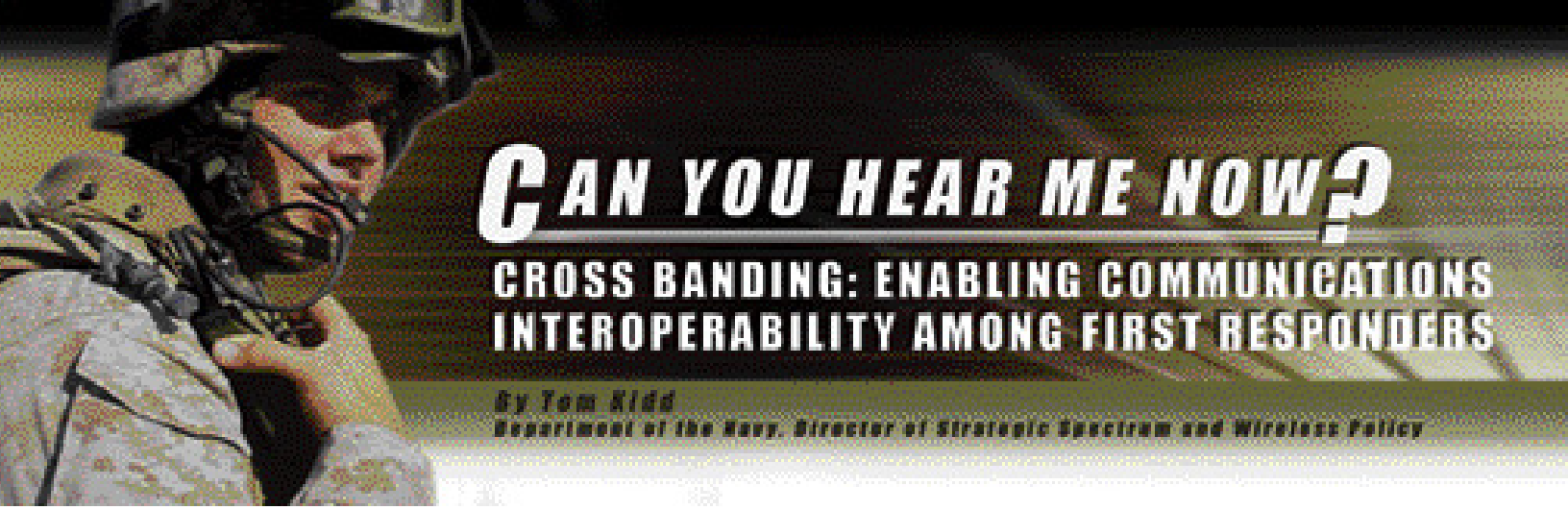
Capt. Roy Petty – Commanding Officer, Navy Cyber Defense Operations Command

Lt. Bobby Carmickle with Robert J. Carey.

Capt. Roy S. Petty

Navy Exchange Service Command Payment Card Industry Compliance Project Team.

DON CIO Rob Carey encourages the DON IM/IT workforce to read for professional development. His recommendations include:
Wikinomics: How Mass Collaboration Changes Everything by Don Tapscott and Anthony D. Williams
The SPEED of Trust: The One Thing That Changes Everything by Stephen M.R. Covey
Leadership is an Art by Max DePree
The 17 Indisputable Laws of Teamwork by John C. Maxwell
Rule Number Two by Dr. Heidi Kraft



CAN YOU HEAR ME NOW?

CROSS BANDING: ENABLING COMMUNICATIONS INTEROPERABILITY AMONG FIRST RESPONDERS

By Tom Kidd
Department of the Navy, Director of Strategic Spectrum and Wireless Policy

Interoperable communications between federal first responders and non-federal first responders is a vital capability that must be pursued by the Department of the Navy (DON) because Navy and Marine Corps installations have a close, cooperative relationship with adjacent federal, state and local first responders. Ensuring interoperable communications for police, fire, emergency medical services, and other first responder services, is a challenging endeavor that can be achieved and ultimately betters the posture and capabilities of the DON.

Interoperable communications for federal, state and local first responders provide significant benefits in crisis management operations where immediate communications can save lives and prevent the loss of property. But ensuring interoperable communications is a complex process that involves a number of factors, including communications control and coordination of radio frequencies.

Coordination of federal and non-federal radio frequencies used for first responders is not exceedingly difficult; however, there can be challenges emplacing necessary agreements and determining technological configurations that are essential to interoperability.

Preparation is the key to successful interoperability. Interoperability plans and agreements should be preprogrammed, and the spectrum (radio frequencies) required to support these operations should be identified and allocated before an incident requiring interoperability is encountered.

Ad hoc plans and solutions are more likely to result in communication shortfalls than solutions that were pre-planned and ready for implementation.

The first step in attaining interoperability is understanding how spectrum is allocated and may be shared and used within first responder agencies. U.S. spectrum governance was purposefully created to protect federal and non-federal spectrum equities; however, the role of the federal agency first responder in domestic emergencies has increased dramatically over the past few decades.

The U.S. radio frequency spectrum is allocated among federal and non-federal services, and use is governed by similar yet different organizations. The use of federal radio frequencies is governed by the National Telecommunications and Information Administration, while non-federal spectrum use is governed by the Federal Communications Commission.

The NTIA and FCC both recognize and support the use of spectrum for interoperable communications between federal and non-federal first responders.

Federal radio frequency users include the departments of the Army, Navy and Air Force, U.S. Coast Guard, and the departments of Justice and the Interior. Sharing federal radio frequencies between federal first responders requires only agency to agency coordination. Agencies are not required to obtain frequency assignments to share the system provided that there is a federal agency that has obtained a federal radio frequency assignment, and that agency consents to other federal agency use.

Federal agencies can obtain frequency assignments in frequency bands allocated exclusively for non-federal use; however, this action requires NTIA and FCC approval and generally requires significant coordination time to ensure that the NTIA and the FCC can support a given frequency assignment. Information on establishing this type of interoperability can be found in paragraph 8.2.48 of NTIA's Manual of Regulations and Procedures for Federal Radio Frequency Management. Resulting frequency assignments are granted with the provision that no harmful interference will be caused to the service rendered by non-federal stations, present or future.

State, local and tribal governments, as well as commercial and private radio users, are examples of non-federal users. Similar to federal agency use of non-federal frequency assignments, non-federal frequency assignments may be authorized in a frequency band solely allocated for federal use. And, similar to federal organizations obtaining non-federal frequency assignments, the assignments require FCC and NTIA coordination. Resulting assignments are provisioned so that no harmful interference will be caused to the service rendered by federal stations, present or future.

Akin to the coordination time for federal frequency assignments in non-federal frequency allocations, non-federal assignments in federal frequency allocations will often require considerable coordination and time.

A common misconception concerning interoperable communications is that all parties must operate on the same frequency. But there are radio systems and equipment that can "cross band" a frequency from one frequency band to a frequency from a different band. Cross banding is transparent to users. Equipment of this type provides many advantages and eliminates the associated challenges of coordinating, acquiring and maintaining "out of band" frequency assignments.

Cross band capabilities allow federal users to operate on frequencies managed by the NTIA, and non-federal users to operate on frequencies managed by the FCC while providing interoperable communications without the use of a single frequency. As such, cross band capabilities minimize the complexity of frequency coordination and use while providing fully interoperable communications. CHIPS

Tom Kidd is the DON director of Strategic Spectrum and Wireless Policy. In addition to "Can You Hear Me Now?" – he also authors the recurring CHIPS series "Going Mobile."

Knowledge Management on a Joint Task Force

KM can be successful without expensive technology and with simple changes

By Cmdr. Diane Boettcher

During Operation Torch, the World War II invasion of North Africa, Gen. George Patton directed operations about 20 hours each day. This means that if he made a decision every other minute, he was making 600 decisions a day. We can estimate that as 60 seconds to be briefed, 30 seconds to discuss options with his staff, and then 30 seconds to issue orders.

Knowing that his primary source for information was the telephone, along with letters and a radio network, we can assume that current commanders have access to exponentially more information. *However, they do not have access to more decision-making time*. You could say they are still limited to 600 decisions a day.

As early as 2002, Gartner Research reported that 90 percent of business managers believe they suffered from information overload. Information overload can cause physical stress, as well as poor decisions, due to overconfidence in information that is actually incomplete or inaccurate.

U.S. military leaders share the same concerns about information overload that business managers do. Following a recent exercise, an intelligence officer told me, "I still don't know what knowledge management is, but I know we needed some. I had no time for analysis, only to check my e-mail and develop slides for the next briefing."

KM as Information Sharing

Knowledge management is a discipline that requires organizations to be *deliberate* about how they process knowledge that will be shared with the people who need to know it so they can make better decisions faster.

While we don't manage knowledge, we can manage the people, processes and technology that handle knowledge to maximize sharing. Lately, the phrase "information sharing" has gained prominence in the lexicon and has the added advantage of being quickly and easily understood.

KM Staffing

Most military organizations are finding that their chief knowledge officer (or knowledge management officer) can achieve better results when reporting to the chief of staff or deputy commander vice reporting to a division or department head.

The KMO/CKO should have sufficient rank to avoid being redirected to other efforts. KMOs that are treated as technical support will spend their days solving the command's IT problems rather than identifying and resolving knowledge flow difficulties.

KMOs should also have appropriate background and training. Too often, this position is given to someone who lacks a fundamental understanding of KM principles, who becomes enamored with tools, rather than focusing on the people and process aspects of the organization.

Trained KMOs should be placed in all key boards, centers and cells, but at a minimum in the operations, intelligence, logistics, administrative and training groups. These KMOs will report to the KMO/CKO and have other duties, but they still must be trained to recognize key information and how to share it.

The CKO will work with the J6 (command, control, communications and computer systems) to ensure that the tools provided are appropriate for the KM plan. The J7 (plans and force development) will help train personnel on the processes and tools, while the J1 (manpower and personnel) should identify and recruit the people needed to execute the organization's mission.

It is important to emphasize that KM can be accomplished without technology and begin with simple changes. For example, early KM practitioners recommended locating personnel, who needed to work together, in the same physical proximity. This seems like common sense today, but it wasn't that long ago when all the executives of an organization were on a single floor, middle managers on another, and line personnel somewhere else.

Placing people next to each other increases the potential of random, unanticipated knowledge sharing that can improve an organization's efficiency and effectiveness.

Other KM practices seek to take advantage of the systems already in place. Most e-mail applications, for example, have a variety of features that can improve knowledge sharing without an additional IT investment.

KM on a Joint Task Force Staff

Knowledge management on a joint task force staff focuses primarily on the creation and flow of knowledge within the staff and at key interfaces with higher and lower headquarters.

Many processes and tools exist to help facilitate this flow of knowledge. Among them are the Commander's Critical Information Requirements (CCIRs); the Battle Rhythm; a significant events (SIGACT) log; and even a phone book or contact list. Other processes that need to be supported are building briefs, capturing lessons learned, handling requests for information and tracking actions.

The KM plan must begin with an understanding of the staff structure and their roles and responsibilities. Just as one would first survey the technical architecture of a network before recommending improvements or upgrades, the KMO must survey the cultural architecture of the knowledge network of the staff.

Who do they share information with? Where do they seek information? How do these exchanges occur? Where and when do they take place? This information can be used to build an "as-is" information exchange matrix.

The "to-be" or recommended information exchange matrix can then be developed. This matrix should outline what information should be exchanged, how and when.

Keep in mind when developing this matrix the cultural implications of changes to the existing information exchange mechanisms. For example, a staff that is accustomed to using e-mail as their primary form of communication should receive training and encouragement if they are being asked to move such communications to a portal.

The Battle Rhythm is the information exchange matrix described over time. This rhythm will be a key element of the KM plan and typically hinges on a specific daily action.

The daily update brief that the commander must provide to higher headquarters or a tactical decision to proceed

might be the precipitating event around which the battle rhythm is built.

The rhythm is not carved in stone, but should be modified to meet changing requirements. However, consider the ramifications to lower headquarters before changing any incoming information exchange requirement. Those at the tactical edge may be at the far end of a long whip. Minor battle rhythm changes at the JTF may cause major shifts for tactical users, so be sensitive to user needs.

A significant events log should be maintained where everyone in the JTF can access the information. Embedding the SIGACT log into the processes of the JTF can ensure that it will be part of the process rather than in addition to it.

Requiring extra work of the staff is not an efficient use of their time and is unlikely to be sustained over time. For example, a call for CAS (close air support) might require a SIGACT number before being accepted. This type of process support enforces best practices over time and through staff turnover. Ideally, the information would also be available for historical analysis and data mining.

In the early days of any JTF effort, a phone book is essential for communications. If cell phones are distributed, they must be tracked. The Army often uses a large, printed organizational chart that includes names and contact information.

Known as a "horse blanket," this chart provides a clear view of the organization and whom to contact for various issues. While some think that print documents are an anachronism in the IT age, others have seen an immediate improvement in shared understanding among staff members using such basic documents.

Of course, having a horse blanket doesn't preclude the use of an online directory. External points of contact, particularly with nongovernmental organizations and coalition partners, should be included in any phone book. If these basic tools can be updated and annotated with critical information by staff members, the information is more likely to be accurate and more valuable to users.

Future of KM

Knowledge management at its heart will always be about people and processes. However, tools can help transform the way people institute processes.

Young adults joining the military today are changing the way information is viewed and shared. These "digital natives" are bringing with them an ease and familiarity with technology that is unrivaled. They eagerly network and collaborate often because they understand the innovation and creativity that can occur when users collaborate on a problem.

Digital natives, also called Generation Y or Millennials, grew up using digital technology such as cell phones, home computers and the Internet. They have Facebook and MySpace accounts, iPods, and they instant message. They can text on their cell phones faster than most of their parents can type on a full-size keyboard.

Millennials collaborate with gusto so it is important to leverage their abilities when designing a KM plan. Their enthusiasm for networking can have a positive effect on those in your organization who may not be as proficient or are skeptical about sharing information.

Since knowledge management focuses on people, the organization and training for KM personnel will be critical to the proper execution of a KM plan. As new people join the Defense Department and new technology becomes available, we will need to adapt and adjust KM tools and processes to enable them to capture and share knowledge.

Knowledge management can be the best facilitator for the efficient operation of a joint staff and for helping the commander make the best decisions possible in the challenging environments warfighters operate in today. CHIPS

For more information, contact SPAWAR public affairs at (619) 524-3432.

Cmdr. Diane Boettcher is the commanding officer of SPAWAR Reserve Unit 303 located in Mayport, Fla. In 2007, she was mobilized to the Standing Joint Force Headquarters where she served as knowledge management officer and deployed to Afghanistan.

DON CIO Memo Articulates DON EA Near-Term Strategy

The Department of the Navy Chief Information Officer signed the DON Enterprise Architecture (EA) Strategy Memo in February, a first in a series of memos, to articulate the near-term strategy for continued development of the DON EA.

The memo establishes direction to ensure alignment of all DON, Navy and Marine Corps programs and initiatives to the Joint Staff developed Joint Capabilities Areas.

The DON EA will be developed incrementally, with close coordination between the DON CIO, Assistant Secretary of the Navy for Research, Development and Acquisition (ASN(RDA)) Chief Systems Engineer (CHSENG), DON Deputy CIO (Navy), DON Deputy CIO (Marine Corps) and the DON Chief Management Officer (CMO).

Critical tasks identified in the strategy memo include development of:

✓ A DON EA governance process for compliance, and establishing and enforcing DON EA standards and policies;

✓ An abstract layer of the DON EA to provide senior leaders insight into the contents of the EA;

✓ A DON EA management process to ensure EA efforts align to strategic goals and objectives of the Department; and

✓ A DON EA repository, developed concurrently with a policy to mandate its use, to support the discovery and sharing of authoritative EA products and information.

The DON EA Strategy Memo also identifies the value of ensuring that the DON EA be focused on supporting the major decision processes of the DoD and DON, such as the Defense Acquisition Systems, Planning, Programming, Budgeting and Execution, and Joint Capability Integration and Development Systems (JCIDS) processes.

The DON EA Strategy Memo is applicable to all in-process and future DON architecture development efforts that provide or maintain DON, Navy and Marine Corps capabilities, including associated standards developed under or incident to programs, projects, capabilities, systems and initiatives. CHIPS

To download the DON EA Strategy Memo, go to the DON CIO Web site at www.doncio.navy.mil and search under the Policy tab.

SPAWAR Systems Center Pacific Scientists Distinguished for Career Accomplishments

By SPAWAR Public Affairs

Two Space and Naval Warfare (SPAWAR) Systems Center Pacific employees were recently selected as distinguished Scientists/Technologists (ST). These are senior flag-level positions with a focus on science and technology, similar to the Senior Executive Service. Dr. Roy Axford and Dr. Adi Bulsara are now two of only 41 STs throughout the Navy and are SSC Pacific's first appointments in 20 years.

Approval for an ST position involves a rigorous, competitive nationwide selection process. Appointees must demonstrate depth in research and technical accomplishments in a particular field of study that is supported by publications, patents and national or international recognition.

"Adi and Roy are truly deserving of this national recognition," said Carmela Keeney, SSC Pacific's technical director. "This is a tremendous career milestone and is a reflection of the superb research and development they have done over many years. It is also a significant milestone for the center. We are so happy to have two STs at SSC Pacific."

Bulsara is currently the principal mentor of the eleven-member Advanced Dynamics Research group, which is globally recognized as one of the premier groups for research in nonlinear dynamics and, possibly, the leading group on practical applications. This effort, featured on the cover of *Physics Today* in 1996, led to his being awarded SSC Pacific's highest recognition, the Lauritsen-Bennett award. This work has led to a compact, cheap and sensitive room temperature magnetometer that the Marine Corps is considering as an intrusion sensor.

"We've had seriously dark periods of almost zero funding, but our management realized that we had a good thing going and showed remarkable prescience," said Bulsara. "I'm just happy to be able to give something back to the country, the Navy and SSC Pacific, which have all been very good to my family and me."

Axford is internationally recognized as a leader in Navy satellite communications. In 2004, Axford became the Navy lead for the Ka-band feederlinks portion of Mobile User Objective System and continues to serve in this role today. In addition, he supports an Office of Naval Research funded project on topside electromagnetic interference mitigation using forward error correction methods in digital communications. In June 2005, Axford also received the prestigious Lauritsen-Bennett award for outstanding leadership in improving the quality of Navy optical and radio communications.

"I have been extremely fortunate in my career at the center to work with an assortment of talented individuals," said Axford. "I have put in many long hours, but very few of my achievements have resulted entirely from solo efforts. I am honored to be recognized with the ST promotion."

For more information about SPAWAR, go to http://enterprise.spawar.navy.mil. CHIPS

SPAWAR Systems Center Pacific employees Dr. Adi Bulsara (left) and Dr. Roy Axford were recently selected as distinguished Scientists/Technologists. The appointment for the science and technology community is similar to an appointment in the Senior Executive Service. There are only 41 such appointments throughout the Department of the Navy.

SURFOR Debuts SWO e-Mentor Program

By Naval Surface Forces Public Affairs

Those who have found success in their careers did not do it alone. Along the way they found someone who they respected and who had a positive impact on their personal and professional life. This mentor shared resources, time, experiences and expertise.

Now Surface Warfare Officers (SWO) can establish these relationships over the Internet. The Surface Warfare Officer e-Mentor Program was established Feb. 2 to capitalize on the diversity of talent within the Surface Community. The program encourages sharing SWO values and knowledge throughout the community.

Surface Warriors serve around the globe at the highest operational tempo in history, which creates a challenge for SWOs, junior and senior alike, who need career guidance, but have trouble finding a mentor that can help guide them in their Navy career.

To connect these professionals with a mentor, SURFOR has implemented a mentor matching tool via the Internet to encourage professional development and serve as an information exchange for officers facing daily work and life challenges.

"Our community is widely known for developing leaders by promoting training, practical experience and best practices while giving consideration to the diversity of backgrounds in our Surface Force," said Vice Adm. D.C. Curtis, Commander Naval Surface Forces and Commander, Naval Surface Force, U.S. Pacific Fleet.

"Much of this knowledge is passed along through mentoring, which is the foundation of good leadership," Curtis said.

The e-Mentor program facilitates relationships by utilizing technology and formalizing matches. Knowledge, skills, life and professional experiences are looked at for both mentor and mentee. The tools on the e-Mentor site will then assist SWOs in matching themselves with potential mentors who have similar perspectives or experiences throughout the community.

Beginning Feb. 16, SWOs can go to https://www.3creekmentoring.com/swo_mentoring to create a profile and perform an online mentor search. Mentor profiles will appear, and searches can be narrowed by entering location, experience, designator, and rank information. A preferred mentor is contacted by the mentee, and together they can establish goals and a professional development action plan.

The Web site also has professional articles on mentoring and career guidance and offers progress tracking tools. Once a partnership is established, communications are facilitated through e-mail, face-to-face meetings or teleconferencing. CHIPS

NSTC DEVELOPING NEW VIDEO GAME

New role-playing game enhances a Sailor's critical thinking and problem-solving ability

By Scott A. Thornbloom

Move over Xbox, video computer gaming is coming to the Navy. But unlike popular combative games, such as Halo 3 or Madden NFL 09, this game will be a training tool adapted to a new generation of gaming Sailors.

"This has the look and feel of a first-person role-playing game, but it would be better to call it a training simulation designed to enhance a Sailor's critical thinking, problem solving, decision making and ultimately on-the-job performance," said Rodney Chapman, director of Learning Strategies (N9) at Naval Service Training Command (NSTC).

The new Navy video computer training tool called VESSEL, or Virtual Environments for Ship and Shore Experiential Learning, combines first person role-playing with real-world training and strategy into a computer-based game.

"This is uncharted waters," Chapman said. "We are using game-based technology to supplement instructor-led training. This strategy should lead to improved Sailor readiness and performance where the Navy can introduce real-time fleet concepts to Sailors at various stages of their career. We happen to be starting this effort in Great Lakes; however, the strength of this technology is applicable and will help improve all Sailors no matter how senior or experienced."

Although there are flight simulators for Navy pilots and large bridge simulators for Navy surface officers to learn navigation, VESSEL can be accessed by merely popping a disc into a computer, just like inserting a disc into a PlayStation or Xbox.

Through partnerships, with BBN Technologies; Intelligent Decisions Systems, Inc.; the University of California, Los Angeles; University of Central Florida (UCF); the Office of Naval Research; and Recruit Training Command (RTC), NSTC's N9 department designed the computer-based training tool to be adaptive to enhance learning and build confidence for Sailors who will be handling shipboard operations and casualties such as flooding and firefighting.

Dr. Clint Bowers, a psychology professor at UCF, said the game has an intrinsic quality that motivates young people. "If we can tap that motivation so that Sailors want to go back to their room or compartment and play and learn and not feel they are in a classroom, we think that will be a great thing."

Sailors report to the "Petty Officer of the Watch" on the quarterdeck of their first ship during the virtual introductory story for VESSEL, a new "Virtual Environments for Ship and Shore Experiential Learning" computer game designed to enhance a Sailor's critical thinking, problem solving, decision making and ultimately on-the-job performance. U. S. Navy photo by Scott A. Thornbloom, Naval Service Training Command Public Affairs Office.

Sailors have participated in the game's evaluation since October 2008, and Bowers said they have demonstrated a high level of interest. "It's one thing to build a game, but we need to make sure it works and we are seeing that it is."

The first simulation is designed to have Sailors investigate a space aboard a ship for flooding from a cracked firemain. Just like popular action-packed video games, the scenario begins with a short story to set the stage.

In the game, Sailors find they have transferred from Naval Station Great Lakes to their first ship in Norfolk, Va. After boarding the ship, Sailors enter the game in a first-person role-playing scenario and must report to their repair locker after the general quarters alarm has sounded.

From the repair locker, Sailors are sent as investigators and directed to look for a possible flood in a certain space. Sailors will need to find the space by locating the correct "bulls-eye" (numbered identification outside the space on the bulkhead) and, once found, go into the space where they will find there is flooding from a crack on the firemain. Sailors should then call Damage Control (DC) Central and report the situation.

"A more senior enlisted Sailor might want to shut down the firemain and cut off the water, but that would be wrong in this simulation," Chapman said.

"We want the Sailor to report the flooding to DC Central using the shipboard phone IVCS (Integrated Voice Communications System) in the space, then go back to the repair locker and pick up the equipment they might need [in this case, a jubilee patch], bring the equipment back to the space and properly patch the pipe."

In the simulation there is only one way to seat the jubilee patch, by putting it on the pipe and sliding it from the top down over the crack. If the Sailor doesn't seat the patch correctly, it will come off.

Sailors are graded on how long it takes to report to the repair locker, find the flooded space, report to DC Central, return to the repair locker, and patch the pipe.

If Sailors perform correctly by maneuvering through the game, they would then need to call back to DC Central and make a final report of what they did and how they accomplished the task.

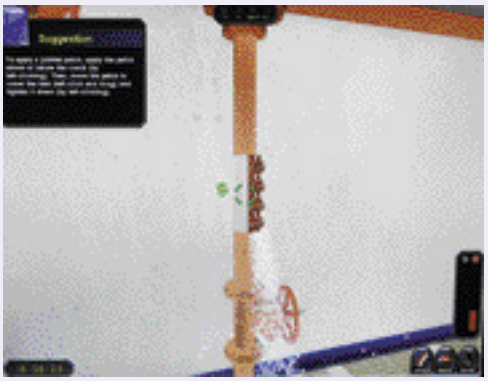
An example of what a Sailor might report would be, "Flooding was secured by properly applying jubilee patch over crack on firemain in space 1-109-2-L, admin berthing. There is two inches of water on deck, or there is no water coming up through the grates. Request dewatering team is sent to compartment."

After a Sailor has made a final report and has been told that a dewatering team has been sent to the space, objectives for the evolution show up on the left side of the computer monitor with a green, yellow or red indicator.

If an objective lights up green, the Sailor has successfully met that objective. If yellow lights up, the recruit completed the objective but performed marginally and could have been faster making reports, getting the right equipment or he or she may have taken too long patching the firemain.

Red means a failure for that particular

During the hands-on-training with Virtual Environments for Ship and Shore Experiential Learning (VESSEL), Sailors talk to Damage Control (DC) Central using a virtual shipboard Integrated Voice Communications System (IVCS) phone to report damage and get further instructions to repair a damaged firemain.



At left, in the VESSEL scenario the ship is in the Persian Gulf, general quarters is sounded, and Sailors must apply a jubilee patch to a damaged firemain. VESSEL provides an adaptable learning experience for young Sailors who are experienced video game players. Below, Seaman Apprentice Melvin Cooks, 18, from East St. Louis, Ill., "plays" VESSEL. Cooks is attending Boatswain's Mate "A" School. U.S. Navy photos by Scott Thornbloom, NSTC public affairs office.

objective, and the actions performed incorrectly will be identified. The Sailor will need to go through the task again.

After the objectives have been graded Sailors will then be directed to an Individual Development Plan (IDP). The plan is based on how well they did and what areas need work. Sailors are then told where to go to receive more instruction on the identified area for improvement.

"This was a great experience,"said Seaman Apprentice Melvin Cooks, age 18, from East St. Louis, Ill. "I think this will help Sailors in here at Great Lakes and in the fleet to strengthen and refresh what they learned at boot camp and in school."

Cooks, a student at Boatswain's Mate "A" School and an early test subject, added that gaming tools, like Battle Stations 21 and VESSEL, help Sailors be more prepared to handle situations and emergencies on board ships and in the fleet.

Chapman called the IDP the most important thing for each Sailor.

"Ultimately, besides the usability of the game, we've put in enhancements with the Individual Development Plan. If I believed they were going to walk away from the test and remember what they were supposed to work on, I'd be sadly mistaken. We are going to deliver an Individual Development Plan with further instruction and training to make them better Sailors," he said.

Early indications of improved Sailor performance are encouraging and impressive, according to Chapman. Two groups of Sailors were selected to participate in a study that required them to secure flooding in a main space on board the Navy's largest training simulator, USS Trayer (Battle Stations 21), a 210-foot long Arleigh Burke-class destroyer, located at Recruit Training Command Great Lakes.

Both groups had basic damage control training but had no previous exposure to the Trayer's internal compartments or design. Only one of the two groups played VESSEL. The Sailors who played VESSEL found the flooded compartment using a bull's-eye, learned from the game, in half the time than the Sailors who didn't play the game (two versus four minutes). Sailors had less than half (eight versus 17) of the communications errors when making reports to DC Central.

Twice as many (50 percent versus 25 percent) non-VESSEL participants repaired the leak without permission and 50 percent of the non-VESSEL participants secured the firemain without permission. No one from the group exposed to VESSEL secured the firemain.

Even though N9 and ONR have been testing the game on recruits from RTC since October 2008, VESSEL is not geared toward passing Battle Stations 21, the final test for a recruit before graduating from the Navy's only boot camp. Battle Stations 21 is conducted on board Trayer a week prior to graduation.

"We didn't specifically build this for Battle Stations 21 because we knew there would be a far-reaching benefit to the rest of the Navy enterprise. We purposely built this [VESSEL] so it could be used at RTC or delivered to TSC (Training Support Center) and other training or shipboard commands fleet-wide. The educational outcome and benefits [of VESSEL] will be consistent if you are in recruit training or out in the fleet. Whether you are a recruit, a bluejacket, chief or officer; this will benefit all Sailors."

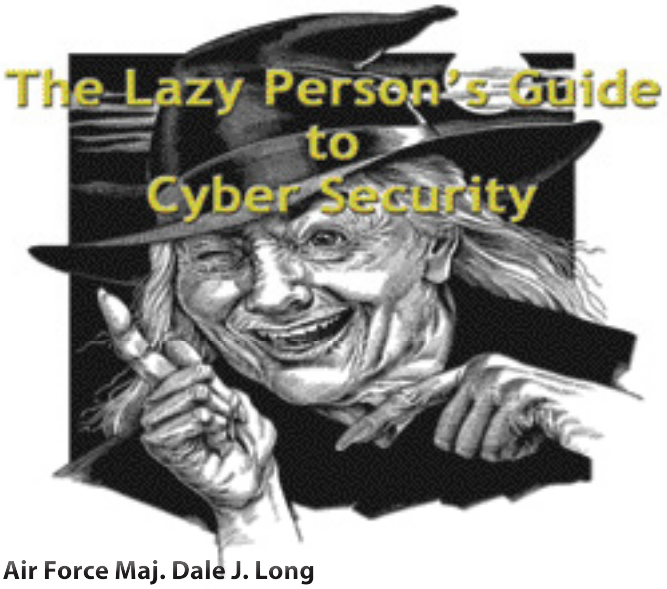
The N9 team is working with ONR to build more scenarios to accompany the flooding model. They are exploring adding oil on top of the flooded water and placing hot electric wires and personnel casualties in the space.

"We are going to add firefighting to it as another training opportunity and continue to build out to be an enterprise-wide learning tool," Chapman said.

Chapman hopes both delayed-entry personnel, as well as Sailors in the fleet, will use VESSEL as another training tool.

"We are entering an era where we are demanding more from our Sailors and they have to master things in a shorter period of time. We no longer have the luxury to put Sailors through long periods of training." CHIPS

For more information NSTC public affairs office, at (847) 688-2201.



By Retired U.S. Air Force Maj. Dale J. Long

Ding, Dong, the Witch is Dead …

Well, one of them is, at least in theory. I am pleased to report that someone seems to have figured out how to kill a botnet. And not just any botnet, but the Storm botnet, a wicked system alleged to have infected more than 1 million computers during its existence.

A team of researchers from Bonn and RWTH Aachen universities analyzed the notorious Storm botnet and developed an application that links itself into the peer-to-peer (P2P) structure of a Storm worm network. Once there, it can divert drones to a new server controlled by the cleanup crew which can then issue commands to the Storm drones.

The server would direct the drones to download a special cleaning program that would remove Storm from the computer. Researchers think that their system will be able to dismantle a network of more than 100,000 drones without any danger of the central cleaning server collapsing under the load or suffering distributed denial of service attacks from botnet operators.

There is, however, one slight catch: employing this system might violate various national laws against unauthorized access to third-party computers or data tampering. In Germany, the home of the research team, they could face two years of imprisonment for unlawfully deleting, suppressing, making unusable or changing third-party data.

Other nations, including the United States, have similar provisions. In addition to criminal charges, you have to consider civil liability in case the cleanup application accidentally turns the computers into large, polycarbonate silicon boat anchors.

But all is not lost, even if the cleanup application is never deployed. In September 2008, a California-based Internet service provider (ISP), Atrivo/Intercage, long alleged to be associated with the equally infamous "Russian Business Group" cyber crime collective, was disconnected from the Internet by its upstream provider. Some declared this the final nail in the coffin for the Storm worms because Atrivo allegedly hosted Storm's control servers.

However, despite concerted efforts to clean it up, Storm is still thought to have 100,000 or so zombies still at large, albeit without much in the way of a command and control (C2) structure. And even if someone wipes Storm completely off the face of the Internet tomorrow, there are other botnets waiting to try and fill 95 percent of our inboxes with spam. But at least security researchers are working to combat them.

Brave New Botnets

Shortly after Atrivo was turned off, hosting provider McColo — a network that allegedly absorbed many of the cyber roaches fleeing Atrivo's shutdown — was also unplugged by its upstream providers in November. That stung, among others, the Srizbi botnet, another massive spam-producing operation with an estimated 450,000 infected computers. Organizations that monitor Internet traffic noted anywhere from a 50 to 75 percent reduction in e-mail spam on the day McColo was taken down.

Another less sophisticated but virulent botnet that ran into trouble in 2008 was Bobax (aka Kraken), which has been around since 2004. In April 2008, SecureWorks, a network security provider, reported that Bobax was the largest spam botnet with 185,000 active bots. Unfortunately for Bobax, it relied on a single hosting provider for its connectivity. In December 2008, that provider killed all of Bobax's control servers.

However, much like cockroaches, you can never really be completely sure that a botnet is dead, so it remains to be seen if Bobax is dead or merely waiting for new masters.

Unfortunately, that is pretty much where the good news ends. The reductions in spam from disconnecting Atrivo and McColo were temporary because other, more sophisticated botnets using encrypted or custom communication protocols, which are not dependent on a single host provider for C2, have moved in to fill the gaps. Botnets named Cutwail, Rustock, Donbot and Ozdok, each reportedly controlling more than 100,000 compromised clients, will be sending spam as fast as they can generate it.

And there are more waiting in line behind them, including a botnet called Waledac that seems to be a rewrite of Storm. Much as we like to kill off botnets, they not only seem to have the resilience of cockroaches; they breed like them too. As quickly as security and legal teams find and eliminate botnets, botnet owners develop more sophisticated systems.

Instead of using a single host for C2, they distribute over many hosts. Bot herders are hardening their systems with encryption both for communications and botnet clients.

They are also programming their zombie clients to send traffic to many Web addresses, in addition to their C2 servers, to make finding the actual control servers more difficult.

So, though there has been some progress fighting botnets, overall, we still don't have a pretty picture. For more on the botnet outlook for 2009, allow me to recommend an article, "Spam Botnets to Watch in 2009" on the SecureWorks Web site at: www.secureworks.com.

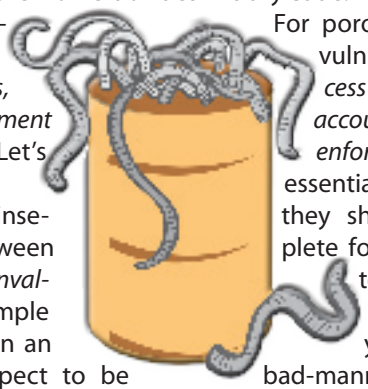
The Top 25

In addition to trying to kill botnets outright, another strategy is to deny them new zombies. With that in mind, computer security experts from 35 international, academic, corporate and government organizations released a list in January

of the 25 most dangerous programming errors that create security vulnerabilities and how to avoid or fix them.

The U.S. federal government was represented by members of the National Security Agency's Information Assurance Division and the Department of Homeland Security's National Cyber Security Division.

The group divided the vulnerabilities into three main categories: *insecure interaction between components, risky resource management* and *porous defenses*. Let's look at a few of them.



The most common insecure interaction between components is called *invalid input validation*. A simple example of this is when an identifier that you expect to be numeric contains letters. If the system is not designed to reject improper input, it may become confused when attacked by input modified in unexpected ways.

Another potential avenue for insecure interactions uses Structured Query Language. An SQL injection attack occurs when an attacker tries to modify the SQL code that is used to communicate with databases.

For example, if a system uses SQL queries in authentication security controls, an attacker can attempt to alter the logic of those queries to bypass security. Other uses for SQL injection include modifying queries to steal, corrupt or otherwise change data.

Cross-site scripting (XSS) is a dangerous vulnerability associated with Web applications. In XSS, attackers try to add JavaScript or other browser-executable content into a Web site. When users browse a tainted page, their browser executes the malicious script. This attack is particularly effective if the infected site is a high traffic, trusted site. Visitors are "infected" as they "drive by" the site whether or not they download any content.

The No. 1 risky resource management vulnerability is the "Failure to Constrain Operations within the Bounds of a Memory Buffer," or buffer overflow, for short. A buffer overflow happens when a program attempts to put more data in a buffer than it can hold or attempts to put data in a memory area outside of the boundaries of a buffer. This can, as with other attacks, confuse the system enough so that the attacker can then do other nefarious things.

When malware permits read or write operations on memory located outside of an allocated range, an attacker may be able to access/modify sensitive information, cause the system to crash, alter the intended control flow, or execute arbitrary code.

For porous defenses, the three top vulnerabilities are: *improper access controls, secret hard-coded accounts* and *client-side security enforcement*. Poor access controls essentially allow users to do things they shouldn't, like viewing complete folder directories. An analogy to this disaster waiting to happen is like inviting people to your house and having a few bad-mannered guests peek into your medicine cabinet or wander into your study and snoop in your checkbook.

Standard system passwords are not new, though most of them are also not particularly secret. Most systems come with a default administrator account, and you can bet any hacker worth his salt will either have a list of default passwords for popular systems or will have purchased (or stolen) a copy of the system to figure out the default account.

Smart system administrators change these defaults as soon as a system is installed. However, some developers have been known to write secret accounts into their systems, thus leaving a somewhat permanent vulnerability available to any hacker who can find it.

Client-side security enforcement problems occur when you trust client software to perform security checks on behalf of your server. Unfortunately, it leaves the keys to system access in the client software — an open invitation for hackers to reverse-engineer the client and write their own version — which, of course, will omit the security controls.

Combined with some of the previously mentioned authentication, authorization and input validation issues, this can be quite dangerous. While client-side validation may be convenient at some level, it is not a good security practice.

These are just general descriptions of only a few of the common weaknesses described in the report. For a complete report on the conference, more detailed descriptions of all 25 vulnerabilities, and discussion of how to avoid them, please see the conference report on the Sans Institute Web site at www.sans.org.

My Top Six List

So, where does cyber security go from here? Based on what we have been discussing for the last year and what we are seeing in cyberspace, here are my "Top Six" cyber security predictions for the next few years.

Stealthier Attack Methods. Given the evolution in botnet technology toward decentralization and encryption, the bot herders that survive the current worldwide purge will be those who fly under the radar. Early botnets thrived because people either did not know they existed — or did not believe they existed.

Dedicated security professionals, many of them working together, amassed enough evidence to start the gradually increasing avalanche of cyber security and legal activity that is burying the less agile botnets.

However, like using an antibiotic that kills only 99 percent of virulent germs, the remaining 1 percent may remain resistant to what worked the first time and transform into something even more predatory. The next generation of botnets may not be as easy to detect.

Smarter Attacks. Brute force attacks, a method of defeating a cryptographic scheme by systematically trying a large number of possibilities, which can include a dictionary attack, while still possible, are being supplanted by more intelligent attack methods, like collecting publicly available documents and files from a target and analyzing their metadata to develop attack profiles.

You can see a basic example of this by opening any common document format, going to the "File" menu and clicking on "Properties." This will reveal what the file knows about itself, including the software version used to prepare it and possibly the author's name and organization.

This can help a hacker on two levels: (1) He now knows the software the organization uses, which gives him a potential technical attack vector if that software has vulnerabilities, and (2) It may give him names and other organizational information to plan a social engineering attack.

Autonomous Evolution. Military troops prefer fire-and-forget weapons because they can launch an attack without being exposed to enemy fire. They can just pull the trigger and a smart weapon takes care of the rest.

Hackers like this paradigm too. I offer as an example the recent attacks by a worm known as Downadup or Conficker. This rapidly spreading worm may be a tool for building a huge new botnet, according to security researchers. It spreads itself, and then it prevents infected PCs from being cleaned up.

Once implanted, the worm searches out nearby servers and executes a brute force password-breaking program. It also spreads itself to any shared hard drives. What's more, it makes a copy of itself on any device plugged into a USB port, such as any thumb drives, music players or digital cameras. When that infected device is later plugged into another PC, it infects that machine, which then begins to similarly spread more infections.

Big Bulls-Eyes. Mark Twain once commented that if you put all your eggs in one basket you should watch that basket very carefully.

With the centralization of data stores over the last decade, much of our important financial, corporate and government information is migrating to fewer and larger network and storage systems.

However, as we discovered with banks and the Wild West, when you gather together large sums of money in one place, you attract thieves. News stories these days are full of reported breaches into centralized credit card databases and other sensitive information repositories.

It is a bit like the situation that confronted Lt. Gen. Walter Short, the Army Air Corps commander responsible for the defense of U.S. military installations in Hawaii at the time of the Japanese attack on Pearl Harbor Dec. 7, 1941.

Based on prevailing belief that local Japanese sympathizers were a greater threat than a Japanese air attack, Short made, what was arguably a reasonable decision. Short rationalized that clustering parked aircraft would be easier to protect against saboteurs than dispersing the aircraft.

Unfortunately, his strategy turned out to be tragically wrong. On Short's orders, the Army parked planes in such a way as to make them more vulnerable to aerial attack.

Compartmentalizing information protects it at the expense of making it less convenient to use. Centralizing information makes it easier to use, but at the potential risk of giving away the entire store if someone gains unauthorized access.

We should not limit ourselves to thinking in three-dimensional terms, as Short strategized in positioning Army aircraft, because in cyberspace, it does not matter where things are physically located.

The people who will make a lot of money in the next decade will be the ones who figure out how to give compartmentalized information the same ease of use as centralized information, so that authorized users will still have access — without compromising security.

If hackers can decentralize their botnets to defend against detection and elimination while still maintaining centralized command and control, then we should be able to do the same to defend our information resources.

System Lockdowns. On the positive side, it appears that network administrators and security professionals are making progress in securing systems. Internet service providers are now looking at security less as an inconvenience and as more of a way to protect their customers.

In one example reported by Spamhaus, a major ISP, allegedly home to 25 percent of e-mail spam that originated inside the United States, moved its Web-based e-mail traffic from Port 25, which does not require authentication, to Port 587, which requires an account ID and password to send e-mail.

Port 25 was a traditional channel for large organization e-mail communications, but because of its lack of authentication it is a favorite target for junk e-mail relays once a computer is infected.

While moving to Port 587 will not stop a zombie from sending spam, it will require that zombie to identify itself to the system, which helps in tracking and cleanup.

Yes, We Can. This last prediction is less a trend than a hope. The last thing most users want to see is one more computer security control that disables or locks down what they consider useful functionality on their PC or network.

Granted, there have been good reasons to clamp down because lots of bad people really are out to get us and get into our systems. But the "fortress network" mentality is almost totally defensive, and you do not win football games, or wars, with only defensive maneuvers.

With that in mind, I am seeing, in some circles, a move toward positive security, where people can try things on their computers using a balanced approach to security and flexibility. As we get better at protecting our networks, I hope to see more flexibility achieved through innovative security measures.

Final Words

The Internet is much like a human body: a large organism with a huge number of interdependent component parts, including hardware and software, networks and users, control mechanisms and communications links. It is, thanks to its basic design, mostly self-healing, routing around damage and regulating the flow of data.

Computer security, in the endgame, will not depend on securing individual systems, but in securing all systems. It will not depend solely on technical measures, but also on diplomatic, legislative, judicial and political change at home and abroad.

As long as viruses, bacteria, cockroaches and bot herders have a place to hide, we will get colds, staph, bugs in the kitchen and junk e-mail.

While we, personally, may not be able to effect all the global technical, political, diplomatic, legislative and legal changes required, we can still do our best to help shine lights into dark corners and make the world a little less safe for the roaches in the system. CHIPS

Until next time, Happy Networking and Good Hunting!

Long is a retired Air Force communications officer who has written regularly for CHIPS since 1993. He holds a master of science degree in information resources management from the Air Force Institute of Technology. He currently serves as a telecommunications manager in the Department of Homeland Security.

Enterprise Software Agreements
Listed Below

The **Enterprise Software Initiative (ESI)** is a Department of Defense (DoD) initiative to streamline the acquisition process and provide best-priced, standards-compliant information technology (IT). The ESI is a business discipline used to coordinate multiple IT investments and leverage the buying power of the government for commercial IT products and services. By consolidating IT requirements and negotiating Enterprise Agreements with software vendors, the DoD realizes significant Total Cost of Ownership (TCO) savings in IT acquisition and maintenance. The goal is to develop and implement a process to identify, acquire, distribute and manage IT from the enterprise level.

Additionally, the ESI was incorporated into the Defense Federal Acquisition Regulation Supplement (DFARS) Section 208.74 on Oct. 25, 2002, and DoD Instruction 500.2 in May 2003.

Unless otherwise stated authorized ESI users include all DoD components, and their employees including Reserve component (Guard and Reserve) and the U.S. Coast Guard mobilized or attached to DoD; other government employees assigned to and working with DoD; nonappropriated funds instrumentalities such as NAFI employees; Intelligence Community (IC) covered organizations to include all DoD Intel System member organizations and employees, but not the CIA nor other IC employees unless they are assigned to and working with DoD organizations; DoD contractors authorized in accordance with the FAR; and authorized Foreign Military Sales.

For more information on the ESI or to obtain product information, visit the ESI Web site at http://www.esi.mil/.

Software Categories for ESI:

Asset Discovery Tools

Belarc

Belmanage Asset Management - Provides software, maintenance and services.

Contractor: ***Belarc Inc.*** (W91QUZ-07-A-0005)

Authorized Users: This BPA is open for ordering by all Department of Defense (DoD) components and authorized contractors.

Ordering Expires: 30 Sep 11

Web Link: https://ascp.monmouth.army.mil/scp/contracts/viewcontract.jsp?cNum=W91QUZ-07-A-0005

BMC

Remedy Asset Management - Provides software, maintenance and services.

Contractor: ***BMC Software Inc.*** (W91QUZ-07-A-0006)

Authorized Users: This BPA is open for ordering by all Department of Defense (DoD) components and authorized contractors.

Ordering Expires: 29 May 09 (Please call for extension information.)

Web Link: https://ascp.monmouth.army.mil/scp/contracts/viewcontract.jsp?cNum=W91QUZ-07-A-0006

Carahsoft

Opsware Asset Management - Provides software, maintenance and services.

Contractor: ***Carahsoft Inc.*** (W91QUZ-07-A-0004)

Authorized Users: This BPA is open for ordering by all Department of Defense (DoD) components and authorized contractors.

Ordering Expires: 19 Nov 09

Web Link: https://ascp.monmouth.army.mil/scp/contracts/viewcontract.jsp?cNum=W91QUZ-07-A-0004

DLT

BDNA Asset Management - Provides asset management software, maintenance and services.

Contractor: ***DLT Solutions Inc.*** (W91QUZ-07-A-0002)

Authorized Users: This BPA has been designated as a GSA SmartBUY and is open for ordering by all Department of Defense (DoD) components, authorized contractors and all federal agencies.

Ordering Expires: 01 Apr 13

Web Link: https://ascp.monmouth.army.mil/scp/contracts/viewcontract.jsp?cNum=W91QUZ-07-A-0002

Patriot

BigFix Asset Management - Provides software, maintenance and services.

Contractor: ***Patriot Technologies Inc.*** (W91QUZ-07-A-0003)

Authorized Users: This BPA has been designated as a GSA SmartBUY and is open for ordering by all Department of Defense (DoD) components, authorized contractors and all federal agencies.

Ordering Expires: 08 Sep 12

Web Link: https://ascp.monmouth.army.mil/scp/contracts/viewcontract.jsp?cNum=W91QUZ-07-A-0003

Business and Modeling Tools

BPWin/ERWin

BPWin/ERWin - Provides products, upgrades and warranty for ERWin, a data modeling solution that creates and maintains databases, data warehouses and enterprise data resource models. It also provides BPWin, a modeling tool used to analyze, document and improve complex business processes.

Contractor: ***Computer Associates International, Inc.*** (W91QUZ-04-A-0002)

Ordering Expires: Upon depletion of Army Small Computer Program (ASCP) inventory

Web Link: https://ascp.monmouth.army.mil/scp/contracts/compactview.jsp

Business Intelligence

Business Objects

Business Objects - Provides software licenses and support for Business Objects, Crystal Reports, Crystal Enterprise and training and professional services. Volume discounts range from 5 to 20 percent for purchases of software licenses under a single delivery order.

Contractor: ***EC America, Inc.*** (SP4700-05-A-0003)

Ordering Expires: 04 May 10

Web Link: http://www.gsaweblink.com/esi-dod/boa/

Mercury

Mercury Software - Provides software licenses, training, technical support and maintenance for Mercury Performance Center, Mercury Quality Center, Mercury IT Governance Center and Mercury Availability Center.

Contractor: ***Spectrum Systems, Inc.*** (SP4700-05-A-0002)

Ordering Expires: 21 Feb 09 (New agreement to be awarded. Please call for information.)

Web Link: http://www.spectrum-systems.com/contracts/esi-hp.htm

COTS Systems Integration Services

COTS Systems

COTS Systems Integration Services - Provides the configuration; integration; installation; data conversion; training; testing; object development; interface development; business process reengineering; project management; risk management; quality assurance; and other professional services for COTS software implementations. Ordering under the BPAs is decentralized and is open to all DoD activities. The BPAs offer GSA discounts from 10 to 20 percent. Firm-fixed prices and performance-based contracting approaches are provided to facilitate more efficient buying of systems integration services. Five BPAs were competitively established against the GSA schedule. Task orders must be competed among the five BPA holders in accordance with DFARS 208.404-70 and Section C.1.1 of the BPA. Acquisition strategies at the task order level should consider that Section 803 of the National Defense Authorization Act for 2002 requirements were satisfied by the BPA competition.

Contractors:

Accenture LLP (N00104-04-A-ZF12); (703) 947-2059

BearingPoint (N00104-04-A-ZF15); (703) 747-8854

Computer Sciences Corp. (N00104-04-A-ZF16); (856) 988-4505

Deloitte Consulting LLP (N00104-04-A-ZF17); (571) 480-7272

IBM Corp. (N00104-04-A-ZF18); (703) 424-7581

Ordering Expires: 03 May 09 (Please call for information about follow-on contract.)

Web Link: http://www.it-umbrella.navy.mil/contract/enterprise/erp_services/erp-esi.shtml

Database Management Tools

Microsoft Products

Microsoft Database Products - See information under Office Systems on page 58.

Oracle (DEAL-O)

Oracle Products - Provides Oracle database and application software licenses, support, training and consulting services. The Navy Enterprise License Agreement is for database licenses for Navy customers. Contact the Navy project manager.

Contractors:

Oracle Corp. (W91QUZ-07-A-0001); (703) 364-3351

DLT Solutions (W91QUZ-06-A-0002); (703) 708-9107

immixTechnology, Inc. (W91QUZ-08-A-0001); Small Business; (703) 752-0632

Mythics, Inc. (W91QUZ-06-A-0003); (757) 284-6570

TKC Integration Services, LLC (W91QUZ-09-A-0001); (571) 323-5584

Ordering Expires:

Oracle: 30 Sep 11
DLT: 1 Apr 13
immixTechnology: 26 Aug 11
Mythics: 18 Dec 11
TKCIS: 29 Jun 11

Authorized Users: This has been designated as a DoD ESI and GSA SmartBUY contract and is open for ordering by all U.S. federal agencies, DoD components and authorized contractors.

Web Link: https://ascp.monmouth.army.mil/scp/contracts/compactview.jsp

Special Note to Navy Users: On Oct. 1, 2004, and May 6, 2005, the Navy established the Oracle Database Enterprise License, effective through Sept. 30, 2013. The enterprise license provides Navy shore-based and afloat users to include active duty, Reserve and civilian billets, as well as contractors who access Navy systems, the right to use Oracle databases for the purpose of supporting Navy internal operations. Navy users in joint commands or supporting joint functions should contact the NAVICP Mechanicsburg contracting officer at (717) 605-3210 for further review of the requirements and coverage.

This license is managed by the Space and Naval Warfare Systems Center (SPAWARSYSCEN) Pacific DON Information Technology (IT) Umbrella Program Office. The Navy Oracle Database Enterprise License provides significant benefits including substantial cost avoidance for the Department. It facilitates the goal of net-centric operations by allowing authorized users to access Oracle databases for Navy internal operations and permits sharing of authoritative data across the Navy enterprise.

Programs and activities covered by this license agreement shall not enter into separate Oracle database licenses outside this central agreement whenever Oracle is selected as the database. This prohibition includes software and software maintenance that is acquired:

a. as part of a system or system upgrade, including Application Specific Full Use (ASFU) licenses;
b. under a service contract;
c. under a contract or agreement administered by another agency, such as an interagency agreement;
d. under a Federal Supply Service (FSS) Schedule contract or blanket purchase agreement established in accordance with FAR 8.404(b)(4); or
e. by a contractor that is authorized to order from a Government supply source pursuant to FAR 51.101.

This policy has been coordinated with the Office of the Assistant Secretary of the Navy (Financial Management and Comptroller), Office of Budget.

Web Link: http://www.it-umbrella.navy.mil/contract/enterprise/deal/Oracle/oracle.shtml

Sybase (DEAL-S)

Sybase Products - Offers a full suite of software solutions designed to assist customers in achieving Information Liquidity. These solutions are focused on data management and integration; application integration; Anywhere integration; and vertical process integration, development and management. Specific products include but are not limited to: Sybase's Enterprise Application Server; Mobile and Embedded databases; m-Business Studio; HIPAA (Health Insurance Portability and Accountability Act) and Patriot Act Compliance; PowerBuilder; and a wide range of application adaptors. In addition, a Golden Disk for the Adaptive Server Enterprise (ASE) product is part of the agreement. The Enterprise portion of the BPA offers NT servers, NT seats, Unix servers, Unix seats, Linux servers and Linux seats. Software purchased under this BPA has a perpetual software license. The BPA also has exceptional pricing for other Sybase options. The savings to the government is 64 percent off GSA prices.

Contractor: ***Sybase, Inc.*** (DAAB15-99-A-1003); (800) 879-2273; (301) 896-1661

Ordering Expires: 30 Sep 09

Authorized Users: Authorized users include personnel and employees of the DoD, Reserve components (Guard and Reserve), U.S. Coast Guard when mobilized with, or attached to the DoD and nonappropriated funds instrumentalities. Also included are Intelligence Communities, including all DoD Intel Information Systems (DoDIIS) member organizations and employees. Contractors of the DoD may use this agreement to license software for performance of work on DoD projects.

Web Link: https://ascp.monmouth.army.mil/scp/contracts/compactview.jsp

Enterprise Application Integration

Sun Software

Sun Products - Provides Sun Java Enterprise System (JES) and Sun StarOffice. Sun JES products supply integration and service-oriented architecture (SOA) software including: JES Identity Management Suite; JES Communications Suite; JES Availability Suite; JES Web Infrastructure Suite. Sun StarOffice supplies a full-featured office productivity suite.

Contractors:

Commercial Data Systems, Inc. (N00104-08-A-ZF38); Small Business; (619) 569-9373

Dynamic Systems, Inc. (N00104-08-A-ZF40); Small Business; (801) 444-0008

World Wide Technology, Inc. (N00104-08-A-ZF39); Small Business; (301) 731-8105

Ordering Expires: 24 Sep 12

Web Link:
http://www.it-umbrella.navy.mil/contract/enterprise/application_integration/SUN/index.shtml

Enterprise Architecture Tools

IBM Software Products

IBM Software Products - Provides IBM product licenses and maintenance with discounts from 1 to 19 percent off GSA pricing. On June 28, 2006, the IBM Rational Blanket Purchase Agreement (BPA) with immixTechnology was modified to include licenses and Passport Advantage maintenance for IBM products, including: IBM Rational, IBM Database 2 (DB2), IBM Informix, IBM Trivoli, IBM Websphere and Lotus software products.

Contractor: ***immixTechnology, Inc.*** (DABL01-03-A-1006); Small Business; (800) 433-5444

Ordering Expires: 26 Jun 09 (Please call for extension information.)

Web Link: https://ascp.monmouth.army.mil/scp/contracts/compactview.jsp

Enterprise Management

CA Enterprise Management Software (C-EMS2)

Computer Associates Unicenter Enterprise Management Software - Includes Security Management; Network Management; Event Management; Output Management; Storage Management; Performance Management; Problem Management; Software Delivery; and Asset Management. In addition to these products there are many optional products, services and training available.

Contractor: ***Computer Associates International, Inc.*** (W91QUZ-04-A-0002); (800) 645-3042

Ordering Expires: 22 Sep 09

Web Link: https://ascp.monmouth.army.mil/scp/contracts/compactview.jsp

Citrix

Citrix - Provides a full range of Metaframe products including Secure Access Manager, Conferencing Manager, Password Manager, Access Suite & XP Presentation Server. Discounts range from 2 to 5 percent off GSA Schedule pricing plus spot discounts for volume purchases.

Contractor: ***Citrix Systems, Inc.*** (W91QUZ-04-A-0001); (772) 221-8606

Ordering Expires: 22 May 09 (Please call for extension information.)

Web Link: https://ascp.monmouth.army.mil/scp/contracts/compactview.jsp

Microsoft Premier Support Services (MPS-2)

Microsoft Premier Support Services - Provides premier support packages to small and large-size organizations. The products include Technical Account Managers, Alliance Support Teams, Reactive Incidents, on-site support, Technet and MSDN subscriptions.

Contractor: ***Microsoft*** (W91QUZ-09-D-0038); (980) 776-8283

Ordering Expires: 31 Mar 10

Web Link: https://ascp.monmouth.army.mil/scp/contracts/compactview.jsp

NetIQ

NetIQ - Provides Net IQ systems management, security management and Web analytics solutions. Products include: AppManager; AppAnalyzer; Mail Marshal; Web Marshal; Vivinet voice and video products; and Vigilant Security and Management products. Discounts are 10 to 8 percent off GSA schedule pricing for products and 5 percent off GSA schedule pricing for maintenance.

Contractors:

NetIQ Corp. (W91QUZ-04-A-0003)

Northrop Grumman - authorized reseller

Federal Technology Solutions, Inc. - authorized reseller

Ordering Expires: 5 May 09 (Please call for extension information.)

Web Link: https://ascp.monmouth.army.mil/scp/contracts/compactview.jsp

ProSight

ProSight - Provides software licenses, maintenance, training and installation services for enterprise portfolio management software. The software product provides the enterprise with a suite of solution specific applications for Capital Planning and Investment Control (CPIC) Budgeting (OMB 300/53); CPIC Process (Select/Control/Evaluate); IT Governance; FISMA (Federal Information Security Management Act) and Privacy Compliance; Project Portfolio Management; Application Rationalization; Research and Development (R&D) and Product Development; Asset Management; Grants Management; Vendor and Service Level Agreement Management; and Regulatory Compliance. ProSight products have been designated as a DoD ESI and GSA SmartBUY. The BPA award has been determined to be the best value to the government and; therefore, competition is not required for software purchases. Discount range for software is from 8 to 39 percent off GSA pricing, which is inclusive of software accumulation discounts. For maintenance, training and installation services, discount range is 3 to 10 percent off GSA pricing. Credit card orders are accepted.

Contractor: ***ProSight, Inc.*** (W91QUZ-05-A-0014); (503) 889-4813

Ordering Expires: 19 Sep 11

Web Link: https://ascp.monmouth.army.mil/scp/contracts/compactview.jsp

Quest Products

Quest Products - Provides Quest software licenses, maintenance, services and training for Active Directory Products, enterprise management, ERP planning support and application and database support. Quest software products have been designated as a DoD ESI and GSA SmartBUY. Only Active Directory Products have been determined to be the best value to the government and; therefore, competition is not required for Active Directory software purchases. Discount range for software is from 3 to 48 percent off GSA pricing. For maintenance, services and training, discount range is 3 to 8 percent off GSA pricing.

Contractors:

Quest Software, Inc. (W91QUZ-05-A-0023); (301) 820-4800

DLT Solutions (W91QUZ-06-A-0004); (703) 709-7172

Ordering Expires:
Quest: 14 Aug 10
DLT: 01 Apr 13

Web Links:
Quest
https://ascp.monmouth.army.mil/scp/contracts/viewcontract.jsp?cNum=W91QUZ-05-A-0023
DLT
https://ascp.monmouth.army.mil/scp/contracts/viewcontract.jsp?cNum=W91QUZ-06-A-0004

Telelogic Products

Telelogic Products - Offers development tools and solutions which assist the user in automation in the development life cycle. The major products include DOORS, SYNERGY and TAU Generation. Licenses, maintenance, training and services are available.

Contractors:

Bay State Computers, Inc. (N00104-07-A-ZF48); Small Business Disadvantaged; (301) 352-7878, ext. 116

Spectrum Systems, Inc. (N00104-07-A-ZF46); Small Business ; (703) 591-7400

Ordering Expires:
Bay State Computers, Inc.: 4 Aug 10
Spectrum Systems, Inc.: 31 Jul 10

Web Link: http://www.it-umbrella.navy.mil/contract/enterprise/telelogic/telelogic.shtml

Enterprise Resource Planning

Digital Systems Group

Digital Systems Group - Provides Integrated Financial Management Information System (IFMIS) software that was designed specifically as federal financial management system software for government agencies and activities. The BPA also provides installation, maintenance, training and professional services.

Contractor: *Digital Systems Group, Inc.* (N00104-04-A-ZF19); (215) 443-5178

Ordering Expires: 31 Aug 10

Web Link: http://www.it-umbrella.navy.mil/contract/enterprise/erp_software/dsg/dsg.shtml

Oracle

Oracle - *See information provided under Database Management Tools on page 54.*

RWD Technologies

RWD Technologies - Provides a broad range of integrated software products designed to improve the productivity and effectiveness of end users in complex operating environments. RWD's Info Pak products allow you to easily create, distribute and maintain professional training documents and online help for any computer application. RWD Info Pak products include Publisher, Administrator, Simulator and OmniHelp. Training and other services are also available.

Contractor: *RWD Technologies* (N00104-06-A-ZF37); (609) 937-7628

Ordering Expires: Effective for term of the GSA FSS Schedule

Web Link: http://www.it-umbrella.navy.mil/contract/enterprise/erp_software/rwd/rwd.shtml

SAP

SAP Products - Provides software licenses, software maintenance support, information technology professional services and software training services.

Contractors:

SAP Public Services, Inc. (N00104-08-A-ZF41); Large Business; (202) 312-3515

Advantaged Solutions, Inc. (N00104-08-A-ZF42); Small Business; (202) 204-3083

Carahsoft Technology Corporation (N00104-08-A-ZF43); Small Business; (703) 871-8583

Oakland Consulting Group (N00104-08-A-ZF44); Small Business; (301) 577-4111

Ordering Expires: 14 Sep 13

Web Link: http://www.it-umbrella.navy.mil/contract/enterprise/erp_software/sap_products/sap_hdr.shtml

Information Assurance Tools

Data at Rest Solutions BPAs offered through ESI/SmartBUY

The Office of Management and Budget, Defense Department and General Services Administration awarded multiple contracts for blanket purchase agreements (BPA) to protect sensitive, unclassified data residing on government laptops, other mobile computing devices and removable storage media devices.

These competitively awarded BPAs provide three categories of software and hardware encryption products — full disk encryption (FDE), file encryption (FES) and integrated FDE/FES products. All products use cryptographic modules validated under FIPS 140-2 security requirements and have met stringent technical and interoperability requirements.

Licenses are transferable within a federal agency and include secondary use rights. All awarded BPA prices are as low as or lower than the prices each vendor has available on GSA schedules. The federal government anticipates significant savings through these BPAs. The BPAs were awarded under both the DoD's Enterprise Software Initiative (ESI) and GSA's governmentwide SmartBUY programs, making them available to all U.S. executive agencies, independent establishments, DoD components, NATO, state and local agencies, foreign military sales (FMS) with written authorization, and contractors authorized to order in accordance with the FAR Part 51.

Service component chief information officers (CIO) are currently developing component service-specific enterprise strategies. Accordingly, customers should check with their CIO for component-specific policies and strategies before procuring a DAR solution. The Department of the Navy, Army and Air Force will be releasing service-specific DAR guidance for their personnel to follow. Go to the ESI Web site at www.esi.mil for more information.

New Guidance Available for Navy Employees!

The DON CIO has issued an enterprise solution for Navy users purchasing DAR software. Visit the DON CIO Web site at www.doncio.navy.mil and search for "Data at Rest" to read the new policy. The DON awarded MTM Technologies a BPA for purchase of the DON Mobile Armor software bundle. For Navy users, all purchases of DON enterprise DAR solutions must be executed through the enterprise BPA, which can be found on the DON IT Umbrella Program Web site at www.it-umbrella.navy.mil. Procurement of other DAR solutions for Navy users is prohibited. See also page 17 for more information for Navy users. As of press time, other DoD users are not authorized to purchase DAR software because service-specific guidance has not been issued.

Enterprise BPA for Navy DAR Users:

Mobile Armor – ***MTM Technologies, Inc.*** (FA8771-07-A-0301)

Safeboot/McAfee – ***Rocky Mountain Ram*** (FA8771-07-A-0302)

Information Security Corp. - ***Carahsoft Technology Corp.*** (FA8771-07-A-0303)

Safeboot/McAfee – ***Spectrum Systems*** (FA8771-07-A-0304)

SafeNet, Inc. – ***SafeNet, Inc.*** (FA8771-07-A-0305)

Encryption Solutions, Inc. – ***Hi Tech Services, Inc.*** (FA8771-07-A- 0306)

Pointsec/Checkpoint – ***immix Technologies*** (FA8771-07-A-0307)

SPYRUS, Inc. – ***Autonomic Resources, LLC*** (FA8771-07-A-0308)

Credant Technologies – ***GTSI Corp.*** – (FA8771-07-A-0309)

WinMagic, Inc. – ***Govbuys, Inc.*** (FA8771-07-A-0310)

CREDANT Technologies – ***Intelligent Decisions*** (FA8771-07-A-0311)

GuardianEdge Technologies – ***Merlin International*** (FA8771-07-A-0312)

Ordering Expires: 14 Jun 12 (If extended by option exercise.)

Web Link: http://www.esi.mil

McAfee

McAfee - Provides software and services in the following areas: Anti-Virus; E-Business Server; ePolicy Orchestrator; GroupShield Services; IntruShield; Secure Messaging Gateway and Web Gateway.

Contractor: *En Pointe* (GS-35F-0372N)

Ordering Expires: 12 Dec 09

Web Link: http://www.esi.mil

Antivirus Web Links: Antivirus software available at no cost; download includes McAfee, Symantec and Trend Micro Products. These products can be downloaded by linking to either of the following Web sites:

NIPRNET site: https://www.jtfgno.mil/antivirus/av_info.htm
SIPRNET site: http://www.cert.smil.mil/antivirus/av_info.htm

Securify

Securify - Provides policy-driven appliances for network security that are designed to validate and enforce intended use of networks and applications; protects against all risks and saves costs on network and security operations. Securify integrates application layer seven traffic analysis with signatures and vulnerability scanning in order to discover network behavior. It provides highly accurate, real-time threat mitigation for both known and unknown threats and offers true compliance tracking.

Contractor: ***Patriot Technologies, Inc.*** (FA8771-06-A-0303)
Ordering Expires: 04 Jan 11 (if extended by option exercise)
Web Link: http://www.esi.mil

Symantec

Symantec - Symantec products can be divided into 10 main categories that fall under the broad definition of Information Assurance. These categories are: virus protection; anti-spam; content filtering; anti-spyware solutions; intrusion protection; firewalls/VPN; integrated security; security management; vulnerability management; and policy compliance. This BPA provides the full line of Symantec Corp. products and services consisting of over 6,000 line items including Ghost and Brightmail. It also includes Symantec Antivirus products such as Symantec Client Security; Norton Antivirus for Macintosh; Symantec System Center; Symantec AntiVirus/Filtering for Domino; Symantec AntiVirus/Filtering for MS Exchange; Symantec AntiVirus Scan Engine; Symantec AntiVirus Command Line Scanner; Symantec for Personal Electronic Devices; Symantec AntiVirus for SMTP Gateway; Symantec Web Security; and support.

Contractor: ***immixGroup*** (FA8771-05-0301)
Ordering Expires: 12 Sep 10
Web Link: http://var.immixgroup.com/contracts/overview.cfm or www.esi.mil

Notice to DoD customers regarding Symantec Antivirus Products: A fully funded and centrally purchased DoD enterprise-wide antivirus and spyware software license is available for download to all Department of Defense (DoD) users who have a .mil Internet Protocol (IP) address.

Contractor: ***TVAR Solutions, Inc.***
Antivirus Web Links: Antivirus software can be downloaded at no cost by linking to either of the following Web sites:

NIPRNET site: https://www.jtfgno.mil/antivirus/av_info.htm
SIPRNET site: http://www.cert.smil.mil/antivirus/av_info.htm

Xacta

Xacta - Provides Web Certification and Accreditation (C&A) software products, consulting support and enterprise messaging management solutions through its Automated Message Handling System (AMHS) product. The software simplifies C&A and reduces its costs by guiding users through a step-by-step process to determine risk posture and assess system and network configuration compliance with applicable regulations, standards and industry best practices, in accordance with the DITSCAP, NIACAP, NIST or DCID processes. Xacta's AMHS provides automated, Web-based distribution and management of messaging across your enterprise.

Contractor: ***Telos Corp.*** (F01620-03-A-8003); (703) 724-4555
Ordering Expires: 30 Mar 09 (Please call for information about follow-on contract.)
Web Link: http://esi.telos.com/contract/overview/

Lean Six Sigma Tools

iGrafx Business Process Analysis Tools

iGrafx - Provides software licenses, maintenance and media for iGrafx Process 2005 and 2006; Six Sigma and iGrafx Flowcharter 2005 and 2006; iGrafx Process for Six Sigma 2007; iGrafx Flowcharter 2007; Enterprise Central; and Enterprise Modeler.

Contractors:
Softchoice Corporation (N00104-09-A-ZF34); (416) 588-9002 ext. 2072
Softmart, Inc. (N00104-09-A-ZF33); (610) 518-4192
Software House International (N00104-09-A-ZF35); (732) 564-8333
Authorized Users: Open for ordering by all Department of Defense (DoD) components, U. S. Coast Guard, NATO, Intelligence Community and authorized DoD contractors.
Ordering Expires: 31 Jan 14

Web Links:
Softchoice
http://www.it-umbrella.navy.mil/contract/enterprise/iGrafx/softchoice/index.shtml
Softmart
http://www.it-umbrella.navy.mil/contract/enterprise/iGrafx/softmart/index.shtml
Software House International
http://www.it-umbrella.navy.mil/contract/enterprise/iGrafx/shi/index.shtml

Minitab

Minitab - Provides software licenses, media, training, technical services and maintenance for products including Minitab Statistical Software, Quality Companion, and Quality Trainer. It is the responsibility of the ordering officer to ensure compliance with all fiscal laws prior to issuing an order under a BPA, and to ensure that the vendor selected represents the best value for the requirement being ordered (see FAR 8.404).

Contractor: ***Minitab, Inc.*** (N00104-08-A-ZF30); (800) 448-3555 ext. 311
Authorized Users: This BPA is open for ordering by all Department of Defense (DoD) components, U.S. Coast Guard, NATO, Intelligence Community and authorized DoD contractors.
Ordering Expires: 07 May 13
Web Link: http://www.it-umbrella.navy.mil/contract/minitab/minitab.shtml

PowerSteering

PowerSteering - Provides software licenses (subscription and perpetual), media, training, technical services, maintenance, hosting and support for PowerSteering products: Software-as-a-Service solutions to apply the proven discipline of project and portfolio management in IT, Lean Six Sigma, Project Management Office or any other project-intensive area and to improve strategy alignment, resource management, executive visibility and team productivity. It is the responsibility of the ordering officer to ensure compliance with all fiscal laws prior to issuing an order under a BPA, and to ensure that the vendor selected represents the best value for the requirement being ordered (see FAR 8.404).

Contractor: ***immixTechnology, Inc.*** (N00104-08-A-ZF31); Small Business; (703) 752-0661
Authorized Users: All DoD components, U.S. Coast Guard, NATO, Intelligence Community, and authorized DoD contractors.
Ordering Expires: 14 Aug 13
Web Link: http://www.it-umbrella.navy.mil/contract/PowerSteering/PowerSteering.shtml

Office Systems

Adobe Desktop Products

Adobe Desktop Products - Provides software licenses (new and upgrade) and maintenance for numerous Adobe desktop products, including Acrobat (Standard and Professional); Photoshop; InDesign; After Effects; Frame; Creative Suites; Illustrator; Flash Professional; Dreamweaver; ColdFusion and other Adobe desktop products.

Contractors:

ASAP (N00104-08-A-ZF33); (800) 248-2727, ext. 5303

CDW-G (N00104-08-A-ZF34); (703) 621-8211

GovConnection, Inc. (N00104-08-A-ZF35); (301) 340-3861

Insight Public Sector, Inc. (N00104-08-A-ZF36); (301) 261-6970

Ordering Expires: 30 Jun 13

Web Link: http://www.it-umbrella.navy.mil/contract/enterprise/adobe-esa/index.shtml

Adobe Server Products - NEW!

Adobe Server Products - Provides software licenses (new and upgrade), maintenance, training and support for numerous Adobe server products including LiveCycle Forms; LiveCycle Reader Extensions; Acrobat Connect; Flex; ColdFusion Enterprise; Flash Media Server and other Adobe server products.

Contractor:

Carahsoft Technology Corp. (N00104-09-A-ZF31); Small Business; (703) 871-8503

Ordering Expires: 14 Jan 14

Web Link: http://www.it-umbrella.navy.mil/contract/enterprise/adobe-srvr/carahsoft/carahsoft.shtml

Microsoft Products

Microsoft Products - Provides licenses and software assurance for desktop configurations, servers and other products. In addition, any Microsoft product available on the GSA schedule can be added to the BPA.

Contractors:

Dell Marketing L.P. *(formerly ASAP)* (N00104-02-A-ZE78); (800) 248-2727, ext. 5303

CDW-G (N00104-02-A-ZE85); (877) 890-1330

Dell (N00104-02-A-ZE83); (800) 727-1100 ext. 7253702 or (512) 725-3702

GTSI (N00104-02-A-ZE79); Small Business; (800) 999-GTSI ext. 2071

Hewlett-Packard (N00104-02-A-ZE80); (978) 399-9818

Softchoice (N00104-02-A-ZE81); Small Business; (877) 333-7638

Softmart (N00104-02-A-ZE84); (800) 628-9091 ext. 6928

Software House International (N00104-02-A-ZE86); (732) 868-5926

Insight Public Sector, Inc. (N00104-02-A-ZE82); (800) 862-8758

Ordering Expires: 31 Mar 10

Web Link: http://www.it-umbrella.navy.mil/contract/enterprise/microsoft/ms-ela.shtml

Red Hat/Netscape/Firefox

Through negotiations with August Schell Enterprises, DISA has established a DoD-wide enterprise site license whereby DISA can provide ongoing support and maintenance for the Red Hat Security Solution server products that are at the core of the Department of Defense's Public Key Infrastructure (PKI).

The Red Hat Security Solution includes the following products: Red Hat Certificate System and dependencies; Red Hat Directory Server; Enterprise Web Server (previously Netscape Enterprise Server); and Red Hat Fortitude Server (replacing Enterprise Server).

August Schell also provides a download site that, in addition to the Red Hat products, also allows for downloading DISA approved versions of the following browser products: Firefox Browser; Netscape Browser; Netscape Communicator; and Personal Security Manager.

The Red Hat products and services provided through the download site are for exclusive use in the following licensed community: (1) All components of the U.S. Department of Defense and supported organizations that utilize the Joint Worldwide Intelligence Communications System, and (2) All non-DOD employees (e.g., contractors, volunteers, allies) on-site at the U.S. Department of Defense and those not on-site but using equipment furnished by the U.S. Department of Defense (GFE) in support of initiatives which are funded by the U.S. Department of Defense.

Licensed software products available through the August Schell contract are for the commercial versions of the Red Hat software, not the segmented versions of the previous Netscape products that are compliant with Global Information Grid (GIG) standards. The segmented versions of the software are required for development and operation of applications associated with the GIG, the Global Command and Control System (GCCS) or the Global Combat Support System (GCSS).

If your intent is to use a Red Hat product to support development or operation of an application associated with the GIG, GCCS or GCSS, you must contact one of the Web sites listed below to obtain the GIG segmented version of the software. You may not use the commercial version available from the August Schell Red Hat download site.

If you are not sure which version (commercial or segmented) to use, we strongly encourage you to refer to the Web sites listed below for additional information to help you to make this determination before you obtain the software from the August Schell Red Hat download site (or contact the project manager listed below).

GIG or GCCS users: Common Operating Environment Home Page
http://www.disa.mil/gccs-j/index.html
GCSS users: Global Combat Support System
http://www.disa.mil/services/gcss-j.html

Contractor: ***August Schell Enterprises*** (www.augustschell.com)

Download Site: http://redhat.augustschell.com

Ordering Expires: 14 Mar 09 (Please call for extension information.)
All downloads provided at no cost.

Web Link: http://iase.disa.mil/netlic.html

Red Hat Linux

Red Hat Linux - Provides operating system software license subscriptions and services to include installation and consulting support, client-directed engineering and software customization. Red Hat Enterprise Linux is the premier operating system for open source computing. It is sold by annual subscription, runs on seven system architectures and is certified by top enterprise software and hardware vendors.

Contractors:

Carahsoft Technology Corporation (HC1028-09-A-2004)

DLT Solutions, Inc. (HC1013-04-A-5000) This contract will be replaced by a new DLT contract (HC1028-09-A-2003) which is listed below.

DLT Solutions, Inc. (HC1028-09-A-2003)

Ordering Expires:
Carahsoft: 10 Feb 09 (Please call for extension information.)
DLT Solutions: 30 Apr 09 (Please call for information about the follow-on contract.)

Web Link: http://www.esi.mil

WinZip

WinZip - This is an IDIQ contract with Eyak Technology, LLC, an "8(a)" Small Disadvantaged Business (SDB)/Alaska Native Corp. for the purchase of WinZip Standard, a compression utility for Windows. Minimum quantity order via delivery order and via Government Purchase Card to Eyak Technology, LLC is 1,250 WinZip licenses.

Contractor: ***Eyak Technology, LLC*** (W91QUZ-04-D-0010)

Authorized Users: This has been designated as a DoD ESI and GSA SmartBUY contract and is open for ordering by all U.S. federal agencies, DoD components and authorized contractors.

Ordering Expires: 27 Sep 09

Web Link: https://ascp.monmouth.army.mil/scp/contracts/compactview.jsp

Operating Systems

Apple

Apple - Provides Apple Desktop and Server Software, maintenance, related services and support as well as Apple Perpetual Software licenses. These licenses include Apple OS X Server v10.5; Xsan 2; Apple Remote Desktop 3.2; Aperture 2; Final Cut Express 4; Final Cut Studio 2; iLife '08; iWork '08; Logic Express 8; Logic Pro 7; Mac OS X v10.5 Leopard; QuickTime 7 Pro Mac; and Shake 4.1 Mac OS X. Software Maintenance, OS X Server Support, AppleCare Support and Technical Service are also available.

Contractor: ***Apple, Inc.*** (HC1047-08-A-1011)

Ordering Expires: 10 Sep 11

Web Link: http://www.esi.mil

Sun (SSTEW)

SUN Support - Sun Support Total Enterprise Warranty (SSTEW) offers extended warranty, maintenance, education and professional services for all Sun Microsystems products. The maintenance covered in this contract includes flexible and comprehensive hardware and software support ranging from basic to mission critical services. Maintenance covered includes Sun Spectrum Platinum, Gold, Silver, Bronze, hardware only and software only support programs.

Contractor: ***Dynamic Systems*** (DCA200-02-A-5011)

Ordering Expires: Dependent on GSA Schedule until 2011

Web Link: http://www.ditco.disa.mil/hq/contracts/sstewchar.asp

Research and Advisory BPA

Research and Advisory Services BPAs provide unlimited access to telephone inquiry support, access to research via Web sites and analyst support for the number of users registered. In addition, the services provide independent advice on tactical and strategic IT decisions. Advisory services provide expert advice on a broad range of technical topics and specifically focus on industry and market trends. BPA listed below.

Gartner Group (N00104-07-A-ZF30); (703) 378-5697; Awarded 01 Dec 2006

Ordering Expires: Effective for term of GSA contract

Authorized Users: All DoD components. For the purpose of this agreement, DoD components include: the Office of the Secretary of Defense; U.S. Military Departments; the Chairman of the Joint Chiefs of Staff; Combatant Commands; the Department of Defense Office of Inspector General; Defense Agencies; DoD Field Activities; the U.S. Coast Guard; NATO; the Intelligence Community and Foreign Military Sales with a letter of authorization. This BPA is also open to DoD contractors authorized in accordance with the FAR Part 51.

Web Link: http://www.it-umbrella.navy.mil/contract/r&a/gartner/gartner.shtml

Section 508 Tools

HiSoftware 508 Tools

HiSoftware Section 508 Web Developer Correction Tools - Includes AccRepair (StandAlone Edition), AccRepair for Microsoft FrontPage, AccVerify for Microsoft FrontPage and AccVerify Server. Also includes consulting and training support services.

Contractor: ***HiSoftware, DLT Solutions, Inc.*** (N00104-01-A-Q570); Small Business; (888) 223-7083 or (703) 773-1194

Ordering Expires: 31 Aug 10

Web Link: http://www.it-umbrella.navy.mil/contract/508/dlt/dlt.shtml

Warranty: IAW GSA schedule. Additional warranty and maintenance options available. Acquisition, Contracting and Technical fee included in all BLINS.

The DON IT Umbrella Program offers great customer service

Go to the Web sites listed below to learn more:

www.it-umbrella.navy.mil

www.itec-direct.navy.mil

www.esi.mil

UNITED STATES NAVY ETHOS

WE ARE THE UNITED STATES NAVY, OUR NATION'S SEA POWER - READY GUARDIANS OF PEACE, VICTORIOUS IN WAR.

WE ARE PROFESSIONAL SAILORS AND CIVILIANS - A DIVERSE AND AGILE FORCE EXEMPLIFYING THE HIGHEST STANDARDS OF SERVICE TO OUR NATION, AT HOME AND ABROAD, AT SEA AND ASHORE.

INTEGRITY IS THE FOUNDATION OF OUR CONDUCT; RESPECT FOR OTHERS IS FUNDAMENTAL TO OUR CHARACTER; DECISIVE LEADERSHIP IS CRUCIAL TO OUR SUCCESS.

WE ARE A TEAM, DISCIPLINED AND WELL-PREPARED, COMMITTED TO MISSION ACCOMPLISHMENT. WE DO NOT WAVER IN OUR DEDICATION AND ACCOUNTABILITY TO OUR SHIPMATES AND FAMILIES.

WE ARE PATRIOTS, FORGED BY THE NAVY'S CORE VALUES OF HONOR, COURAGE AND COMMITMENT. IN TIMES OF WAR AND PEACE, OUR ACTIONS REFLECT OUR PROUD HERITAGE AND TRADITION.

WE DEFEND OUR NATION AND PREVAIL IN THE FACE OF ADVERSITY WITH STRENGTH, DETERMINATION, AND DIGNITY.

WE ARE THE UNITED STATES NAVY.

DEPARTMENT OF THE NAVY
COMMANDING OFFICER
SPAWARSYSCEN ATLANTIC
CHIPS MAGAZINE
9456 FOURTH AVE
NORFOLK, VA 23511 - 2130
OFFICIAL BUSINESS

PERIODICAL POSTAGE AND FEES PAID NORFOLK, VA AND ADDITIONAL MAILING OFFICE
SSC ATLANTIC
CHIPS MAGAZINE
USPS 757-910
ISSN 1047-9988